Award Number: 47GFDA22F0035
PIID Number 47QFDA21Q0094

Strengths Maintenance Management System (SMMS) & Reserve Component Management System-Guard (RCMS-G) Systems Support Services

for

U.S. Army National Guard (ARNG)

Issued by:
National Capital Region (NCR), Contracting Operations Division (COD)
1800 F Street, NW
Washington, DC 20405

08/10/2022

SECTION C: DESCRIPTION OF SERVICES (STATEMENT OF WORK)

C.1 BACKGROUND

The Army National Guard (ARNG) Personnel (hereinafter referred to as "G1") is responsible for creating, managing, and executing all manpower and personnel plans, programs, and policies across all the ARNG Directorates. The Strength Maintenance Management System (SMMS) and the Reserve Component Manpower System-Guard (RCMS-G) are two systems used to support and enhance the ARNG G1 decision-making process. This enhanced knowledge from both SMMS and RCMS-G provides a basis for senior leaders as they execute their own strategic vision for the ARNG personnel plans, programs, and policy.

SMMS and RCMS-G provide its users with the ability to readily access the personnel data, extract and integrate the data from multiple sources, refine and improve the data, and package the data for decision makers in a form that illustrates trends and key issues apparent for critical Guard-wide decisions. These decisions can range from recruiting needs or limitations for enlistment to ARNG wide impacts such as the types of units in the ARNG.

C.1.1 PURPOSE

The purpose of this requirement is to provide enhancement services for the SMMS and RCMS-G which includes the incorporation of cybersecurity protocols, advancing systems and technologies, and maintaining overall operational readiness of all applications, modules, and programming.

C.1.2 AGENCY MISSION

To support the ARNG G1 mission, the SMMS and RCMS-G suite of applications and modules were developed to provide ARNG action officers and senior leaders with critical manpower information needed to enhance their decision-making process. SMMS and RCMS-G aggregate data from multiple authoritative data sources and present results in the form of user information, such as standard and customizable reports, configurable dashboards, or data files, which are electronically delivered to authorized locations, or presented via Web portal.

C.2 SCOPE

The SMMS and RCMS-G suite is used to access, gather, and present manpower readiness data that informs ARNG decision makers and senior leaders on the Health of the ARNG. This requirement includes the operations, maintenance, data processing, and analytical support for the SMMS and RCMS-G systems and its users as well as making changes to the system (approximately 2,000 software changes annually) to ensure compatibility with evolving technologies. In the performance of the resulting contract, ARNG expects the Contractor to provide innovative solutions that bring technical and operational improvements to the ARNG and its SMMS and RCMS-G users and customers.

In providing services to SMMS and RCMS-G, the contractor must:

- coordinate its efforts with several other contractors and government organizations,
- maintain agreements with those organizational entities,
- and troubleshoot data quality issues, modify and implement system Interface changes and updates, and modify existing data and data processing as other pertinent systems change (such as: Military Occupational Specialty changes and DFAS Line of Accounting (LOA) changes)

The scope of this contract includes:

1. Maintaining the operational readiness of the SMMS and RCMS-G applications, modules, and interfaces;
2. Maintaining the operating system (OS) of the SMMS and RCMS-G servers in the Primary environment and associated Continuity of Operations Plan (COOP) environment;
3. Maintaining the overall health and Army Compliance of the entire SMMS and RCMS-G environment. Compliance to all Army Enterprise Cloud Management Agency (ECMA) policies and Headquarters

Department of the Army (HQDA) G-1 Personnel Technology and Business Architecture Integration (TBAI) policy and guidance.

4. Supporting data operations by providing ongoing management of data feeds, maintenance of SMMS and RCMS-G metrics, and the processing of production data;
5. Providing changes to SMMS and RCMS-G analytical functions;
6. Providing project management and execution of all changes to the SMMS and RCMS-G applications, modules and interfaces, including the integration of selected ARNG G1 systems into the SMMS and RCMS-G environments;
7. Producing, updating, and maintaining the Business Process Reengineering (BPR), Department of Defense (DoD) Architecture Framework (DoDAF), and Business Enterprise Architecture (BEA) documents for all changes to the SMMS and RCMS-G suite;
8. Identifying and eliminating vulnerabilities to SMMS and RCMS-G and;
9. Achieving and maintaining information assurance and accreditation of the SMMS and RCMS-G systems in accordance with (IAW) DoD and federal standards. The contractor must purchase software licenses in order to fulfill the requirements of this contract. The CO must approve all purchases and sources in writing.

C.3 CURRENT ENVIRONMENT

SMMS and RCMS-G features and capabilities have grown over the years in sophistication and quantity. SMMS and RCMS-G are supported by hardware and software systems that include over 100 different modules, applications, and data sources. SMMS and RCMS-G leverage the Microsoft technology stack and other complementary technologies to enable operational efficiencies. SMMS and RCMS-G expose a graphical user interface and support a large number of concurrent users across many functional and operational areas. SMMS and RCMS-G feature a robust enterprise data warehouse based in Microsoft Structured Query Language (MS SQL) which aggregates sources of information from many disparate systems.

Both systems provide data to and receive data from a multitude of systems, such as the Reserve Component Automation Systems (RCAS), Army Training Requirements and Resources System (ATRRS), Integrated Personnel Pay System - Army (IPPS-A), Total Army Personnel Database-Guard (TAPDB-G), Medical Protection System (MEDPROS), Defense Finance Accounting System (DFAS), and approximately 80 data feeds in total. Most data input to both SMMS and RCMS-G is raw data that indicates the status of Reserve Component personnel and the changes that have occurred to ARNG personnel during the current reporting period. Both SMMS and RCMS-G process these data elements and convert them into useful information for the users.

The output generated may take on many forms, such as a graphical output showing grade and year-of-service profiles, a budget book showing the cost of the manpower program over the Future Years Defense Programs (FYDP), or statistics showing personnel readiness during mobilization.

RCMS-G Data Sources

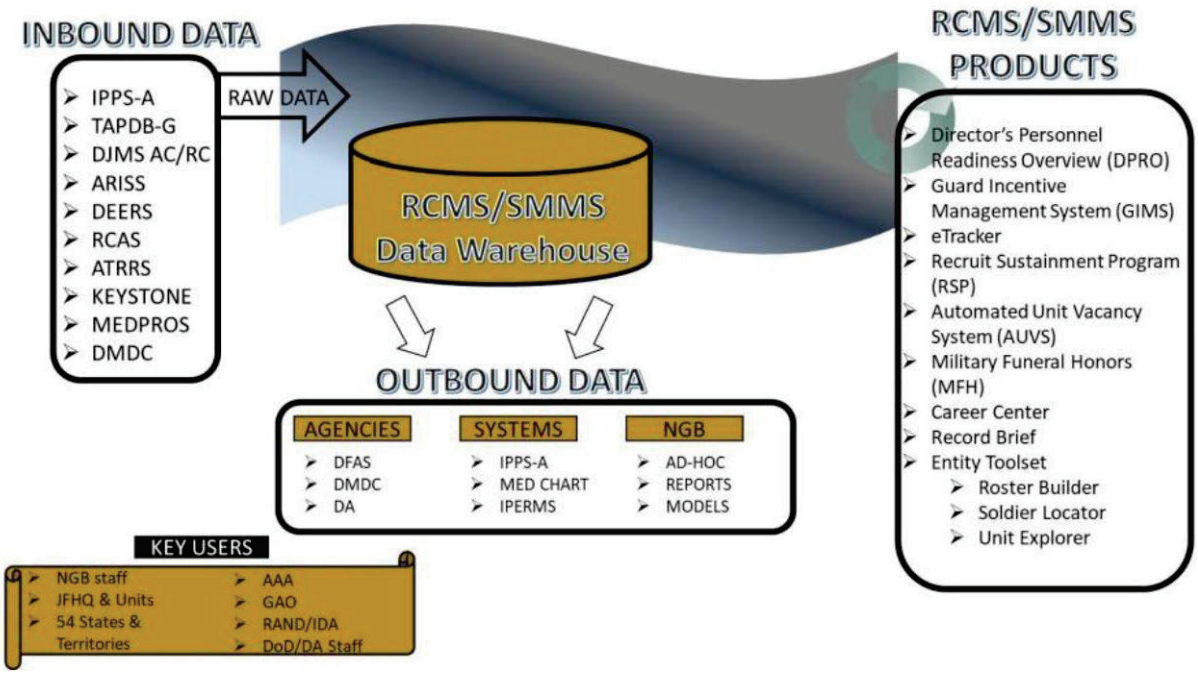

Illustration 1: System Overview of SMMS and RCMS-G

C.4 OBJECTIVES

The overall objectives of this requirement include:

1. Combining all ARNG programs in SMMS and RCMS-G that have been identified as an enduring requirement into a single system (TBAI policy mandate)
2. Incorporate Army HR data changes driven by IPPS-A, AIE, and other Army system modernization efforts into a streamlined and single data warehouse eliminating the need to process data separately for SMMS and RCMS-G that provide real time or close to real time data updates
3. Migrate to a Cloud based hosting environment (currently planned for cArmy Cloud) to include a full spectrum DevSecOps SDLC (may be completed concurrently with objective 1) (ECMA mandate for all ARMY systems)
4. Maximize the efficiencies of the existing SMMS and RCMS-G source code as a low code data driven architecture to increase system capabilities and flexibilities to drive change and produce actionable information

C.5 TASKS

C.5.1 TASK – TRANSITION

The contractor must provide a draft Transition-In Plan to the Government for feedback and provide a final Transition-In Plan as required in Section F. The contractor must ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition as defined in the Service Level Agreements (Appendix A). All transition activities must be completed prior to transition-in POP completion.

Transition-in must require coordination with the incumbent contractor for acceptance of the project. The contractor must perform a joint inventory of all Government-furnished equipment (GFE) with the incumbent contractor and the TPOC or Property Book Officer. All discrepancies and problems must be noted and submitted to the TPOC for resolution in conjunction with the CO, CS, and COR. The contractor must:

- inventory all GFE listed on DA Form 3161.
- have all key personnel available at the project start date, and all critical staff in place within 30 days after

contract award.

- certify to the CO, CS, COR, and TPOC, that all of the contractor's employees meet the training criteria as specified in Sections H.4 through H.7.2.

The key transition objectives for the transition of the SMMS and RCMS-G services to the TO awardee during the transition-in period are to:

1. Minimize transition impact to the user community;
2. Maintain existing service quality and performance levels;
3. Ensure a transparent and seamless transition with no breaks in service availability;
4. Ensure that the IT security posture during transition is maintained at current levels without creating gaps or vulnerabilities.
5. Obtain all GFE required to perform individual duties (Laptops, System Administrator (SA) tokens, ARNG network account, and JSP mainframe access).
6. Assume full system responsibility and be prepared to process all data on time, meeting satisfactory or higher SLA standards.

The contractor must execute the Transition-In Plan in a manner that positions the contractor to successfully assume responsibility for maintaining operational readiness of the SMMS and RCMS-G systems. SMMS and RCMS-G support includes:

1. Standing up the facility;
2. Hiring, training, and obtaining required security clearances, certifications, and system-level access for all staff;
3. Transferring all knowledge required to operate and maintain the environment and to provide user support through the service desk; and
4. Establishing operational relationships with other organizations involved in the operations.
5. Ensuring a fully operational software development environment is transferred and operational, and critical technical support personnel have all required access.

The contractor must manage and perform all tasks required to transition operational support from the incumbent contractor.

It is the responsibility of the contractor to: obtain access to the operational systems, review existing materials to gain an understanding of the current operations and present a comprehensive plan for moving equipment, if needed, in a manner that minimizes disruption to ongoing operations. The contractor must work with the TPOC to obtain this information. The TPOC will not dictate the approach, but must coordinate with the COR to approve all plans.

The SMMS and RCMS-G systems and applications along with their interfaces have been custom developed over many years utilizing a variety of software languages (including: Adobe Flash, ASP.Net, HTML5, Javascript, and others). The current SMMS and RCMS-G source code implementation provides a data driven framework that allows the government a highly configurable low code environment consisting of applications that are META data configurations to produce fast reliable (low code) changes to the required configuration.

C.5.1.1 COORDINATE A PROJECT KICK-OFF MEETING

The contractor must schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government COR. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the Task Order (TO). The meeting will provide the opportunity to discuss system

access, management, security issues, travel authorization, and reporting procedures. No later than (NLT) 5 days after award the contractor will schedule and participate in the Kick-Off Meeting (Section F, Deliverable 1) and deliver a draft Kick-Off Meeting Agenda for review and approval by the Government prior to finalization. At least two days prior to the Kick-Off Meeting the contractor must deliver the final Kick-Off Meeting Agenda (Section F, Deliverable 2). The agenda must include:

a. Points of Contact (POC) for all parties;
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between the contractor and Government);
c. Staffing plan status;
d. Transition-In Plan and discussion (Section F, Deliverable 17);
e. Security discussion and requirements, i.e., building access, badges, Common Access Cards (CACs), telework agreements and limitations;
f. Invoicing requirements; and
g. Review initial Baseline Quality Control Plan (QCP)

The contractor must draft and provide a Kick-Off Meeting Minutes Report documenting the Kick-Off Meeting discussion and any action items. (Section F, Deliverable 3)

Within 5 business days after the Kick-Off Meeting, the contractor must

- submit completed system and system privileged access requests for all key personnel and any other onboarded staff that are identified by the contractor PM as critical to a successful transition. Staff that are on board during the transition must have all required access requests submitted within five days of being identified as critical.
- work directly with all agencies responsible for granting required access.
- ensure that all personnel requiring access are in compliance with DoDD 8140 baseline certifications for the access they are requesting.

The SMMS and RCMS-G PMO will support the contractor's efforts in obtaining access. Failure to obtain the required access will not relieve the contractor from any PWS/SOW tasks.

C.5.1.2 REQUIRED TASKS FOR TRANSITION

Within 15 business days of award, the contractor must establish the operational and support facility, which will house all efforts associated with the technical requirements in this SOW. The proposed facility must meet the minimum requirements. See Section H.

C.5.1.2.1 KNOWLEDGE AND EQUIPMENT TRANSFER

The contractor must provide regular updates on data processing, critical access status, equipment transfer, environment inventory, and a list of all individuals that require elevated/privileged access and those critical to the success of transition will be reported along with the key personnel status at least weekly during the transition-in period in the Weekly Transition Report (Section F, Deliverable 4).

The contractor must:

- Develop and execute a Transition-In Plan;(Section F, Deliverable 17)
- Conduct an inventory of GFE and IT assets;
- Establish management processes and controls necessary to support the transition process;
- Inventory and verify all software titles and license keys settings necessary to operate and maintain the SMMS and RCMS-G systems and environments;
- Inventory all source code, stored procedures, development and administrative tools, and configuration settings, necessary to operate and maintain the SMMS and RCMS-G systems and environments;

- Gain access to and establish an understanding of all Enterprise Mission Assurance Support Service (eMASS) and the various controls, inherited controls, and associated artifacts;
- Assume responsibility for moving GFE equipment from the current SMMS and RCMS-G service provider's to the contractor's facility; and
- Transition tickets to the new ticketing system.
- Gain system environment access and control of software development operations (Including a by name and position list of all Key and Critical personnel and the status of their access requests)
- Establish and demonstrate the ability to host virtual meetings using the ARNG selected medium. Currently the ARNG utilizes the Army ".A365" version of Microsoft Teams .
- Observe data processing and review documentation related to SMMS and RCMS-G data processing processes and procedures

C.5.1.3 SPECIFIC TRANSITION-IN REQUIREMENTS:

The contractor must develop and execute a Transition-In Plan (Section F, Deliverable 17) that includes:

1. Specific tasks to be performed and the resources assigned to them;
2. Task dependencies and relationships;
3. Task duration; and
4. Major milestones.

The transition schedule must be documented within the Transition-In Plan (Section F, Deliverable 17) . The set of tasks must include:

1. Status of Contractor Personnel;
2. Hiring, obtaining/verifying clearance and certifications;
3. Accounts – requesting appropriate accounts from the Government;
4. Training
5. Schedule must include milestones for percentage of staff ready for operations and maintenance (O&M) duties;
6. Facility. This section must document progress towards outfitting the contractor's facility including subcontracts, leases, environmental issues, safety and security in the implementation of their transition strategy;
7. Readiness reviews documenting the capability to operate and maintain all systems processes, procedures, and environments.

The contractor must schedule and conduct weekly status meetings to report and review progress of the transition (Section F, Deliverable 5).

Within the transition-in period, the contractor must demonstrate readiness to proceed prior to Assumption of Operational Responsibility (AOR). The ARNG will review the level to which the contractor was able to accomplish the transitional tasks. The contractor must complete the following within the transition-in period in order to demonstrate readiness and proceed with the task order:

1. Ensure operational readiness of the contractor's facility, including:
    a) Completely outfitted physical office space for all of the contractor's personnel;
    b) Service Desk space;
    c) Telephone system supporting the Service Desk in a manner that supports SLAs outlined in this contract;
    d) Physical access security; and,
    e) Connectivity to SMMS and RCMS-G and associated networks and environments (e.g., internet access, network access, and CAC).
2. Perform a demonstration of the functionality of the contractor-provided ticketing system to the TPOC and COR for approval.

3. Secure all user privileges and access needed.
4. Successfully execute (30) daily, (5) weekly, and (2) monthly processing activities with limited Government support or intervention
5. Successfully support data processing during the transition-in period to include two End of Month (EOM) processing periods and one Quarterly period.

C.5.1.4 SMMS and RCMS-G Data Processing Guide (DPG)

The contractor must observe all data processing during the transition-in period and compare actions performed to the actions described in the DPG. The contractor must annotate and document all additional information required to successfully complete data processing in the DPG Delta Report (Section F, Deliverable 6). The DPG is a "living document" and is sufficient for an experienced and trained Database Administrator (DBA) to successfully complete data processing as required at the time of this contract. The DPG is not a simple or a fully complete step by step guide that would allow an inexperienced DBA to conduct data processing.

C.5.2 TASK 1 – PROGRAM MANAGEMENT

The contractor must provide project management (PM) support under the resulting Task Order (TO). PM support includes the management and oversight of all activities performed by contractor personnel, including subcontractors as applicable, to satisfy the requirements identified in this SOW.

C.5.2.1 PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor must develop and provide a MSR (Section F, Deliverable 7). The MSR must include:

a. Activities during the reporting period by tasks (including ongoing activities, new activities, activities completed, count of releases by category, and progress-to-date on all activities). Each section must start with a brief description of the task.
b. Problems and corrective actions taken including issues or concerns and proposed resolutions to address them.
c. Notification/information about any revoked or expired contractor personnel security clearances.
d. Government actions required.
e. Project schedule with major tasks, milestones, and deliverables; planned and actual start and completion dates for each.
f. Release schedule with the high level requirements that will be completed by module in each of the next three monthly releases and what was released in the last actual monthly release.
g. Cyber security compliance depicting the required and completed scans and all vulnerabilities and risks identified.
h. Summary of trips taken, conferences attended, and attach Trip Reports (defined in 3.5.1.5) to the MSR for the reporting period.
i. Invoice and cost reporting as requested by the COR or TPOC.

C.5.2.2 CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager (PM) must convene a monthly Technical Status Meeting with Government stakeholders (Section F, Deliverable 8). The purpose of the meeting is to ensure all stakeholders are informed of the monthly activities and MSR, SLA performance measurements review, and to provide an opportunity to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM

must provide minutes of these meetings to attendees within 2 business days after the meeting (Section F, Deliverable 9). These meeting minutes must include

- meeting attendance,
- all priorities,
- identified problems and any recommended courses of action,
- opportunities and recommended courses of action,
- decisions made, and
- due out action items.
- Any nonconformance to any SLA or PRS must also be annotated with the reason for nonconformance and when the nonconformance will be brought back to a minimally acceptable level of conformance.

The Contractor must be equipped to hold meetings virtually or in-person at the request of the Government.

C.5.2.3 PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor must document all support requirements in a draft PMP for TPOC and COR review (Section F, Deliverable 10). The final PMP must incorporate TPOC and COR comments. (Section F, Deliverable 11).

The PMP must:

a. Contain detailed Standard Operating Procedures (SOPs);
b. Include milestones, tasks, and subtasks required in this TO;
c. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels (work packages level as defined in the Project Management Body of Knowledge) and associated responsibilities and partnerships between Government organizations;
d. Contractor's risk management efforts under this TO including the transition in;
e. Describe in detail the software release and configuration planning schedule (Most modules/applications are currently on a monthly release cycle, however releases that contain only metadata changes are typically more frequent).
f. Describe in detail the contractor's approach to communications, including processes, procedures, and communication approach between the contractor and the Government; and
g. Include the contractor's Quality Control Plan (defined in 3.55.1.6).

C.5.2.4 UPDATE THE PROJECT MANAGEMENT PLAN

The Project Management Plan (PMP) is a living document that must be updated annually. The contractor must work from the approved PMP and must submit updates to the PMP within 30 days of a substantial change (Section F, Deliverable 12) for approval by the TPOC and COR.

C.5.2.5 TRAVEL REQUEST (TR) AND PREPARE TRIP REPORTS

The contractor must submit a TR for each individual participant. All TRs must include the information below in this section required for a Trip Report.

The contractor must submit Trip Reports to the COR for the Contracting Officer's approval, not later than (NLT) five business days after completion of a trip for all long distance travel. Long distance travel is defined as travel over 50 miles outside of the Washington, DC commuting area. Local travel will not be reimbursed. Travel to the Washington D.C. metro area for employees that are approved to telework in the best interest of the government must do so at the contractor's expense. Long Distance Travel for telework employees beyond the 50 mile radius of their normal place of duty is authorized per JFTR to locations other than the Washington D.C. metro area.

The Trip Report (Section F, Deliverable 13) must include:

a. Name(s) and title(s) of personnel who traveled;
b. Dates of travel;
c. Destination(s);
d. Purpose of trip;
e. Cost of the trip;
f. Approval authority; and
g. Summary of events.

The contractor must keep a summary of all long-distance travel, including the name of the employee, location of travel, duration of trip, and Point of Contact (POC) at the travel location. Trip reports must also contain Government approval authority, total cost of the trip, and a detailed description of the purpose of the trip.

C.5.2.6 PROVIDE QUALITY CONTROL MANAGEMENT

The contractor must develop and maintain an effective Quality Control Plan (QCP) to ensure services are performed in accordance with Section C. The contractor must develop and implement procedures to identify and prevent defective services. The contractor's QCP must describe the application of the appropriate methodology for accomplishing TO performance expectations and objectives. The QCP must describe how the appropriate methodology integrates with the Government's requirements.

The QCP must include:

1. Organization and resources. Organization chart and communication interfaces for all personnel performing Quality Control (QC) functions. Identification of the authority of the QCP manager to monitor and control functions, and to implement remedial and preventive actions;
2. Specific inspection techniques and methods tailored to each functional area;
3. Risk Identification and Remediation Plan; and
4. Procedures for corrective action.

The contractor must update the QCP submitted with its quote and then provide a final baseline QCP within 7 days of receiving feedback on the draft QCP from the TPOC and COR (Section F, Deliverable 15). The contractor must periodically update the QCP as required when changes in program processes are identified (Section F, Deliverable 14).

C.5.2.6.1 QUALITY CONTROL RESPONSIBILITIES

The contractor's quality control team must monitor and promote adherence to established SMMS and RCMS-G service levels and schedules by analyzing Performance Requirements Summary (PRS) data, as well as existing policies and procedures.

The contractor's quality control team must:

1. Formulate and enforce internal work quality standards;
2. Ensure users are notified with service request ticket status;
3. Produce and provide performance reports;
4. Conduct periodic performance reviews to improve current operations;
5. Maintain statistical data in order to demonstrate performance trends;
6. Conduct independent quality reviews of closed tickets to ensure they are managed properly;
7. Ensure service request tickets are closed;
8. Prepare training plans for the development of the staff and to improve service support;
9. Identify user training needs based on analysis of tickets;
10. Investigate report statistics and analysis as appropriate;

11. Investigate missed requirements and identify root causes for the non-compliance; and
12. Identify issues (technical, management, or otherwise) that prevent the contractor from meeting the Service Level Agreements (SLAs) and/or other operational goals.
13. Record all quality concerns, issues, and risks in the Integrated Master Schedule (IMS), report all quality non-conformances, and, report all quality non-conformances on a Problem Notification Request (PNR) within two business days of the occurrence or identification of nonconformance whichever occurs first

At the request of the Government, the contractor must provide reports and updates on quality in the requested format to support the Government's surveillance efforts (Section F, Deliverable 16).

C.5.2.6.2 RESERVED

C.5.2.7 OPSEC SOP/PLAN

The contractor must develop an Operational Security (OPSEC) Standard Operating Procedure (SOP)/Plan (Section F, Deliverable 20) and provide it to the TPOC and COR within 30 calendar days of contract kick-off meeting to be reviewed and approved by the responsible Government OPSEC officer. This SOP/Plan must include a process to identify the government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor must implement OPSEC measures as required by the Government. In addition, the contractor must identify an individual who will be an OPSEC coordinator. The Government requires this individual to be OPSEC Level II certified within 90 days of appointment as OPSEC coordinator in accordance with AR 530-1. Contractor must provide a copy of the certification to the COR and TPOC NLT 15 days after completion (Section F, Deliverable 20).

C.5.2.8 STANDARD OPERATING POLICIES AND PROCEDURES (SOP)

The contractor must establish and maintain formalized SOP and operational plans for each process that supports the operation and maintenance of SMMS and RCMS-G.

The contractor must deliver these (new or updated) procedures for review and approval by the Government (Section F, Deliverable 37). All SOPs must be delivered to the Government within 60 days after contract award and the contractor must brief the Government within five business days of the delivery prior to acceptance of the SOP by the Government. Standard operating procedures include:

1. Service Desk and On-site Support; including ticket creation, updates and resolution;
2. Onboarding, account creation and provisioning;
3. Disaster Recovery Plan;
4. Continuity of Operations Plan (COOP) (Section F, Deliverable 29);
5. Crisis Communication Plan;
6. Cyber Incident Response Plan;
7. Backup, Archive, and Recovery;
8. Data Processing Guide (Section F, Deliverable 25);
9. OPSEC SOP/Plan (Section F, Deliverable 20);
10. Cloud Resource Management; and
11. Change Management Plan (Section F, Deliverable 32).

The contractor must update these plans and procedures within 30 calendar days of identifying a change (Section F, Deliverable 38) and the Government reserves the right to reject an SOP for any reason. If rejected, the contractor must resubmit a revised SOP within 10 business days for reconsideration.

C.5.2.9 SYSTEM METADATA TRAINING & CERTIFICATION PLAN

The contractor must prepare a System Metadata Training and Certification Plan (Section F, Deliverable 39) to prepare government individuals to utilize the existing SMMS and RCMS-G software to edit and maintain metadata. The training plan must include all documentation and required skills for select government employees to be trained in

utilizing the existing software to edit the metadata allowing for software changes in the existing low code environment. The MetaData training Plan must be approved by the government prior to the MetaData training and optional CLIN being awarded.

C.5.2.10 SMMS and RCMS-G TRANSITION OUT

The Contractor must develop a Draft Transition-out Plan (Section F, Deliverable 40). The Draft Transition out Plan must be delivered to the CO/COR/TPOC and later revised to incorporate Government feedback into a Final Transition-out Plan (Section F, Deliverable 41). In the Transition-Out Plan, the contractor must identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding:

a. Project management processes.
b. Points of contact.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor must also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition.

The contractor must implement its Transition-Out Plan NLT six months prior to expiration of the TO.

The TPOC will notify the contractor of all outstanding requirements that must be completed prior to task order expiration which would include--

Phase 1: Ninety calendar days prior to the expiration of the task order, the incumbent contractor must deliver to the Government and/or the incoming contractor the SMMS and RCMS-G development and test environments with all associated tools, documents to include previous versions and source code (The development environment is hosted in AWS GovCloud, therefore “deliver” in this context refers to the required access and transfer of ownership, specific date of transfer of ownership must be coordinated and approved by the government so as to minimize the disruption of services, this may be much closer to TOA than 90 days):

1. Production: All work products related to current SMMS and RCMS-G production environment and solution files, team foundation server or any source code related to the application or sub-Applications;

2. Development: All work products used to develop SMMS and RCMS-G environment to include all production release version and solution files, team foundation server or any source code related to the application or sub-Applications; This includes all ARNG specific and any applicable documentation, quick guides, how to guides, developer implementation guidance, functional notes, or “wiki’s” regarding the SMMS and RCMS-G program.
3. Turn over all administrative access information, i.e., service account information, user-name and password, if applicable grant administrative user access to the ARNG at least 60 calendar days prior to the end of the contract;

4. Work with the incoming contractor in transitioning the operational support; and

5. Provide documentation and information as requested by the Government (the contractor must deliver a copy of

all current and relevant system documentation created during the contract).

Phase 2: The contractor in accordance with its phase-out plan must develop and execute an approach to transition program knowledge to the government and incoming contractor. This approach includes SOPs, plans, information papers, and lessons learned. Knowledge transferred must include backup and restoration procedures. The incumbent contractor is not responsible to train the incoming contractor, however the incumbent must make all aspects of the contract available for observation of employees performing the tasks. This includes questions and answers as the incumbent is performing PWS tasks.

C.5.3 TASK 2 – DATA PROCESSING

The contractor must use the Data Processing Guide (Section F, Deliverable 6) to complete all data processing and preprocessing tasks. This document must be updated as processes change, new feeds are added or deleted, and clarifying information is identified.

The contractor must:

1. Receive data from the external sources. Most interfaces require daily data updates. These interfaces are already established with automated processes (see Task 5 for Systems Interface Requirements);
2. Ensure that all expected data sources have delivered their data (via automated data feeds) by the time agreed-upon in the corresponding agreements;
3. Conduct pre-processing of external data feeds to ensure that record counts and file structures are consistent with previous data feeds as a quality control measure, repair and report abnormalities and raise alerts if it appears that any inconsistencies exist and establish new processes for quality control when existing quality control process are not already in place;
4. Load pre-processed data into the SMMS and RCMS-G production Data Warehouse; and
5. Provide the capability to store copies of verified source data in the staging SMMS and RCMS-G databases and store these data copies.
6. Identify and report all changes to inbound data formats, files not received, or non-conforming data received within 12 hours of identification in the Data Processing Status Report (Section F, Deliverable 22).

C.5.3.1 DATA PROCESSING

The contractor must:

1. Create data sets for inclusion into the SMMS and RCMS-G data warehouse, by removing data duplications as identified by the system. Only data records that represent a change or new records must be appended to a historical database for the life of the system thus supporting accurate backward and forward time series analysis and comparisons;
2. Load pre-processed data into the SMMS and RCMS-G production data warehouse; and
3. Close records that need to be closed based on the existence of updated records in the source data. SMMS and RCMS-G never replace any records; rather old records are closed and new records are inserted. For example, if a soldier is promoted, a new record with the promotion information is inserted into the database and the old record is “closed” by populating “end date” of the previous rank

C.5.3.1.1 DATA PROCESSING ERROR RESOLUTION

As issues with the incoming data are identified, the contractor must:

1. Identify and respond to inquiries of data abnormalities;
2. Identify and carry out corrective actions to resolve data abnormalities;
3. Create ad hoc reports using various tools including MS Excel, SQL and MS PowerPoint and other tools to communicate data issues with ARNG leadership and functional experts; and
4. Create resolution methodologies that will minimize data anomalies and invalid or missing data.

C.5.3.2 MAINFRAME OPERATIONS

In addition to data sources identified above, the SMMS and RCMS-G systems process data stored on a Pentagon mainframe. The Pentagon Mainframe exists as part of the Joint Service Provider Enclave and is a shared space with the Army Reserve. Some data shared via an incoming data feed contains both USAR and ARNG data. The contractor must develop a draft MOU (Memorandum of Understanding) to conduct data sharing of incoming data to the mainframe with any third-party vendors.

The contractor must maintain a historical archive of source data files that reside on the Pentagon mainframe. On a frequent basis, the contractor must copy data sets received from SMMS and RCMS-G interfaces to/from the Pentagon mainframe.

The contractor must provide connections to other systems. This applies primarily to a limited number of situations where the SMMS and RCMS-G interfaces do not provide their data sets directly to SMMS and RCMS-G; rather, these data sources send their data to the Pentagon mainframe and SMMS and RCMS-G pull these data sources from the mainframe. An example of such an arrangement is the Defense Manpower Data Center (DMDC), which puts Defense Finance and Accounting Service (DFAS) data onto the Pentagon mainframe.

The contractor must include Mainframe Operations in the Data Process Status Report (Section F, Deliverable 22).

C.5.3.3 UPDATE DATA PROCESSING DOCUMENTATION

The contractor must document all additional information required to successfully complete data processing in the DPG (Section F, Deliverable 25) at the Government's request.

C.5.4 TASK 3 - DATA OPERATIONS

The contractor must:

1. Maintain and change existing automated data quality control processes by verifying and validating anomalies;
2. Use historical information as the basis for conducting analyses to determine if the new data sets are within an acceptable range and meet expected characteristics;
3. Develop metrics using background statistics and linear regression analysis to determine the validity of the data;
4. Perform periodic data checks on the metrics to identify any data abnormalities;
5. Inspect abnormalities in the metrics to determine if the change is expected or might be signaling an anomaly that may exist;
6. Create data sets for inclusion into the SMMS and RCMS-G data stores by removing data duplications as identified by the system;
7. Create resolution methodologies that will minimize data anomalies and invalid or missing data;
8. Identify and carry out corrective actions to resolve data abnormalities and report abnormalities to user;
9. Maintain and change existing automated data quality control processes by verifying and validating anomalies; and
10. Perform periodic data checks on the metrics to identify any data abnormalities.
11. Report Data abnormalities in the Data Processing Status Report (Section F, Deliverable 22).

C.5.4.1 DATA REPROCESSING

Based on historical records, the ARNG anticipates that a small percentage of the data obtained from the external sources will have corruptions that cannot be identified using the standard check and data quality control processes discussed above. These issues are typically caused by mistakes introduced in the data feeds or data processing. When such issues are discovered the contractor must:

1. Work with the owner of the data source to create methods for identifying the corrupted elements in the SMMS and RCMS-G staging database and update the affected records to their correct values;
2. Rerun all standard checks and quality control processes and reload the updated data into the SMMS and

RCMS-G data store following the data fixes to the staging area;
3. Keep historical records of all such events information about the data source, issues, affected date range, fields, and steps taken to resolve the problem;
4. Evaluate these events for inclusion into the standard data verification and quality control processes; and
5. Deliver the results of this analysis and the details about each event to the ARNG as part of the Data Processing Status Report (Section F, Deliverable 22).

C.5.4.2 DATABASE(S) MAINTENANCE

The contractor must manage the performance and availability of these SMMS and RCMS-G databases that comprise the SMMS and RCMS-G Suite data store. The environment is comprised of Microsoft SQL 2008, 2012, and 2014. The contractor must migrate any existing servers to the latest approved Microsoft SQL server database release prior to the existing SQL version causing a security vulnerability.

The structure and size of the SMMS and RCMS-G databases are:

DB Server Name	Capacity (GB)	DB Storage Used (GB)	Databases	Tables	# of SProcs
NGRCA4-RCMSDB01	7771	5380.82	66	10691	8484
NGRCA4-RCMSDB02	5047	2669.38	83	34974	14716
NGRCA4-RCMSDB03	9320	7060.51	27	13341	4264
NGRCA4-SMMSDB01*	11308	5939.08	87*	17102*	24568*
NGRCA4-SMMSDB02	19140.5	14206.68	65	19677	15265
NGRCA4-SMMSDB05	180	32.37	21	386	2739

*24 of the DBs, 4737 of the Tables, and 9906 of the Stored Procedures are for the exercise environments;

The environments must include Development, Test/Staging, Exercise, and Production environments and may be expanded or decreased as necessary to meet SMMS and RCMS-G mission requirements.

The contractor must monitor and resolve performance issues, data access and setup, monitor status of scheduled backups, coordinate and write processes for inbound and outbound data transfers, and create, schedule to run and monitor all required Extracting, Transforming and Loading (ETL) processes per the service level agreements.

The contractor must be responsible for:

1. Developing and maintaining replication processes to ensure accurate and available data in the various production environments; Providing ongoing coordination with software maintenance team(s) for tailored products, modules, and models database and best practices support; Assessing and improving the database performance, mod schema, manage indexes, produce roll up tables and views and alter speed indexes;
2. Monitoring data alerts and then responding and resolving these issues; and,
3. Reporting data discrepancies and improvement processes achieved in the monthly status report 3.5.1.1).

The contractor must update existing and add new metadata to maintain the integrity of ARNG G1 manpower metrics and their relevance to supporting ARNG manpower analysis requirements.

The contractor must modify stored procedures to incorporate business logic as a result of customer driven changes to

policy and practice.

The contractor must provide an Operational Health Report (Section F, Deliverable 21). This report must be delivered monthly and include all relevant statistics and explanations for suboptimal system health, to include a POAM to mitigate all risks.

The contractor must ensure that its notification about unscheduled maintenance is posted no less than 15 minutes before the start of the maintenance.

C.5.4.3 SYSTEM INTERFACES

The contractor must establish and maintain the system interfaces with external modules, systems, applications, and databases. Approximately 40 interfaces exist between SMMS and RCMS-G and external systems. This task is inclusive of adding, modifying, and deleting system interfaces as well as adding, modifying, and deleting supporting system interface agreements.

The contractor must:

- Change inbound/outbound interfaces to support technology changes, data changes and refreshment;
- Develop database schemas and tables to support interface changes;
- Populate new tables to support growing product lines within the RCMS-G database;
- Establish extracts of data to support requests for information from external systems;
- Ensure that all interface agreements between SMMS and RCMS-G are properly implemented;
- Coordinate and work directly with all interface partners to ensure all required information is provided to support all agreements;
- Conduct meetings at least twice monthly with all pertinent parties for any existing or desired interface that is non-compliant with the terms of the interface agreement or any desired data source working toward an interface agreement. Non-compliance must be documented by the contractor in a Interface Agreement Non-compliance Report(Section F, Deliverable 45);
- The contractor must utilize Installation Processing Node (IPN) and/or Cloud Service Provider (CSP) provided Microsoft Structured Query Language (SQL) 2014 or greater and MySQL NetBackup agents to back up and restore Database Servers; and
- Add new, modify existing, and delete obsolete interface agreements as required in the interface lifecycle.

The contractor must archive all active interface agreements approximately 40 times per year and must update existing interface agreements thirty days prior to the TO expiration (Section F, Deliverable 23).

C.5.4.4 DATA WAREHOUSE CONSOLIDATION PLAN

The contractor must prepare a plan to combine the SMMS and RCMS-G data warehouses. The ARNG intends to combine all databases, procedures, and data processing into a single data warehouse. Currently these data warehouses are very similar and contain a substantial amount of inefficiency. The Consolidation Plan must include all required steps and outline key milestones and dependencies for a successful consolidation. This plan must be approved by the government prior to the SMMS and RCMS-G data warehouse consolidation CLIN being exercised. Data Warehouse Consolidation Plan (Section F, Deliverable 56)

C.5.4.5 MAINFRAME CONVERSION PLAN

The contractor must prepare a plan to convert all mainframe processes and backups to MS SQL Server. The ARNG intends to combine all mainframe databases, procedures, and data processing into a single data warehouse. The Mainframe Conversion Plan (Section F, Deliverable 57) must include all required steps and outline key milestones and dependencies for a successful system conversion. This includes a sustainable plan to share data with the Army Reserve. This plan must be approved by the government prior to the Mainframe Conversion CLIN being exercised.

C.5.4.6 IPPS-A CONVERSION PLAN

The contractor must prepare a plan to convert all IPPS-A data into a streamlined and efficient source for close to real time data processing. The ARNG intends to update databases, procedures, and data processing to utilize an IPPS-A subscription service allowing for close to real time data updates. The IPPS-A Conversion Plan (Section F, Deliverable 58) must include all required steps and outline key milestones and dependencies for a successful conversion including a complete data map and stored procedure update to allow for optimal data consumption. This plan must be approved by the government prior to the IPPS-A Conversion CLIN being exercised.

C.5.4.7 HISTORICAL DATA REPROCESSING PLAN

The contractor must prepare a plan that identifies all data anomalies dating back to at least March 1, 2015 and utilizing all available data to establish parameters for this Historical Data Reprocessing. The Historical Data Reprocessing Plan (Section F, Deliverable 59) must include all required steps and outline key milestones and dependencies for successful data reprocessing to include a mitigation plan that minimizes the disruption to users. This must include an in-depth review of each data feed to determine the best Course of Action (COA) for each feed and present the details as part of the plan. This plan must be approved by the government prior to the Historical Data Reprocessing CLIN being exercised.

C.5.5 TASK 4 – CYBER SECURITY AND COMPLIANCE

The contractor must work with Cyber Security Service Providers (CSSP) and other 3rd parties to monitor and respond to cyber threats.

The contractor must:

1. Support 3rd party Security Control Assessments and Validations (SCA-V) by providing all supporting documentation and explanation of artifacts at the Government's request;
2. Perform vulnerability assessments in order to prepare for and in support of systems Security Control Assessments and Validation events;
3. Perform Risk Management Framework (RMF) or current DoD standards assessments of the SMMS and RCMS-G;
4. Perform source code and executable scans of the SMMS and RCMS-G system and ensure that the system meets all NIST and DoD security requirements;
5. Monitor and respond to Information Operations Condition (INFOCON) Levels to comply with the SD 527-1 or current standard required baseline. When the INFOCON level is elevated, document the level change, the needed readiness activities, the completion of those activities, and any issue associated with complying with the INFOCON required steps;
6. Review and identify recommendations for Chief Technology Officers (CTOs), Execution Orders (EXORDS), including necessary waiver requests and POAMS and deploy guidance and procedures for all INFOCON levels and transitions between them;
7. Support implementation of the emerging cyber warfare doctrines, as required;
8. Update documentation and systems such as e-MASS to reflect system compliance with security controls, and architecture;
9. Ensure the environment maintains accreditation under the RMF accreditation and all other requirements to continue receiving a Tenant in Good Standing Certificate. Authorization to Operate, and/or an IATT;
10. Contractor must ensure that the Army Host Based Security System (HBSS), System Center Configuration Manager (SCCM),and Antivirus clients are installed and functional;
11. Coordinate and follow through with all government agencies to ensure all system security and compliance requirements remain compliant and in good standing with DoD policy and guidance;
12. Develop and maintain a MOU with the ARNG G6 that clearly delineates all Responsibilities, Accountability, Consulted partners, and Informational Awareness required for all security and compliance tasks;

13. Plan, Identify, and Coordinate all security and compliance tasks and be responsible for ensuring all requirements are accomplished with limited system interruptions or limitations; and,
14. The contractor must provide an in-process review of Cybersecurity and Compliance to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.5.1 SMMS and RCMS-G SECURITY SUPPORT AND USER ACCESS

The contractor must ensure that all access to the SMMS and RCMS-G environment is CAC enabled. The contractor must ensure that records are tied to the CAC login of the User entering the information in order to send system emails related to the particular record and auditability. The contractor must implement an enterprise approach to roles and permissions management encompassing all modules, data, and web pages tools. The contractor must implement single sign-on (SSO) capability for all modules.

C.5.5.2 SECURITY COMPLIANCE

The contractor must maintain the SMMS and RCMS-G environment to meet all DoD system security standards and system accreditation standards. Assessing Security and Privacy Controls in Federal Information Systems and Organizations is the current standard for selecting security controls in order to meet the Risk Management Framework (RMF) guidelines and all other requirements to continue receiving an Authorization to Operate (ATO) as appropriate.

SMMS and RCMS-G have an RMF categorization as Medium-Medium-Medium.

Security Controls are inherited from Common Control Providers (CCP) and the Army Policy Record.

The contractor is responsible for Implementing Security Controls, Assessing Security Controls, preparing for System Authorization events, and Monitoring Security Controls on a continuous basis.

The contractor must ensure security controls selections are updated in order to ensure the system is updated appropriately to reflect DoD Accreditation and security standards. The contractor will ensure that SMMS and RCMS-G meets the National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) and Federal Information Security Management Act (FISMA) guidelines set forth in the latest versions of the following documents which are available electronically under DoD government websites:

- NIST SP 800-53
- NIST Special Publication 800-53A Rev 4 (or current revision)
- FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- NIST 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347
- NIST 800-129 Guide for Security-Focused Configuration Management of Information Systems
- NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
- FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
- DoDI 5000.2, Operation of the Defense Acquisition Systems

The contractor must document both system security processes and any security incident or threat in the Cyber security section of the Program Management Plan. The contractor must comply with DoD SOP requirements for compromised data breach as listed DoDD 5400.11-R (DoD Privacy Program) and relevant DoDI for policies, and required actions.

The support in this area includes:

1. Ensuring SMMS and RCMS-G application is programmed according to DISA Security Technical Implementation Guidelines (STIGs), SRG, and will run in an environment and on servers that are STIG/Unified Gold Master (UGM) compliant;
2. Validating configurations with an approved Security Content Automation Protocol (SCAP) scanner and provide scan results as eMASS artifacts and provided as requested;
3. Performing vulnerability scans and reviews to identify all patches and updates;
4. Providing automated daily vulnerability assessment and reporting based on asset inventory;
5. Automatically scanning the environment, source code, and stored procedures to identify and remediate vulnerabilities;
6. Automatically generating service tickets for detected vulnerabilities;
7. Aggressively mitigating vulnerabilities to prevent loss of capability, performance, or information, agency block, or other quarantine and/or user access limitations;
8. Providing the security-related support for patch management to include: Testing all security patches provided by the industry and the DoD to ensure they do not have negative impact on the operational systems;
9. Reviewing waiver requests and present recommended actions to the ARNG TPOC;
10. Adding, updating, and deleting system level user accounts for privileged access of government accounts; and
11. Removing dormant accounts based on business rules.

The contractor must maintain a FISMA compliance with no CAT I (30 days to remediate), no CAT II (60 days to remediate) and no CAT III (90 days to remediate) vulnerabilities that have exceeded the remediation time or have a government approved POAM in place to mitigate and remediate findings. (Exploitable vulnerabilities must be mitigated to an acceptable level of risk before being placed on a POAM). Vulnerabilities are not considered remediated until they are eliminated from the training and production environments.

The contractor must update eMASS to reflect the status of security control and vulnerability scans.

The contractor must be responsible for maintaining security control documentation, associating it to controls in eMASS and making it available upon request by the Authorizing Official (AO), Information System Owner (ISO), Information Systems Security Manager (ISSM), Information System Security Officer (ISSO), or an outside agency.

The contractor must monitor ATO records for all SMMS and RCMS-G modules and support the POAM as initiated by the Government. The contractor must update eMASS instances to reflect system status.

The contractor must provide an in-process review of the Cyber Security and Compliance report to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.6 TASK 5 – HELP DESK / SERVICE DESK INFRASTRUCTURE

The contractor must establish a service desk.

The Service Desk Infrastructure must include:

1. Service Desk Ticketing System,
2. Service Desk Call Reporting System,
3. Service Desk Ticket Creation, and
4. Service Desk Managing Tickets.

The contractor must provide the ARNG the ability to view Help Desk Verifiable Closed Tickets on a daily basis (Section F, Deliverable 35).

C.5.6.1 SERVICE DESK TICKETING SYSTEMS

This contractor-provided ticketing system must be used to track and manage user inquiries as well as events reported

though automated systems. In addition, the system must be able to track projects and their approval process.

System must generate the following set of timestamps for each ticket record:

1. Create date and time;
2. Last updated date and time;
3. Resolved date and time; and
4. Closed date and time.

The Service Desk must be located at the contractor's facility.

The contractor must provide and manage a ticketing system, which will be used to manage incident, problem,and service requests reported by the users, SMMS and RCMS-G staff (Government and contractor), or automated sources.

To support service desk operations, the contractor must provide:

1. Assistance with account issues;
2. Assistance with usage of the SMMS and RCMS-G Suite and its features;
3. Troubleshooting;
4. Coordination of resolution efforts; and
5. Grant access to the National Guard Bureau Program Management Team to perform reporting and analysis.

C.5.6.2 SERVICE DESK CALL REPORTING SYSTEM

Service Desk Call Reporting Requirements:

The contractor must provide a web-based reporting system capable of presenting current and historical data about call, email, and web activities.

The contractor-provided repository must be capable of transmitting the above information to a standards-based external database using SQL, Java Database Connectivity (JDBC), and/or Open Database Connectivity (ODBC) interfaces

The reporting tool must have the flexibility to collect data and distribute reports via a 'push' method, 'pull' method, or a combination thereof.

The Call/Contact Type reports must include:

1. Average and longest speed of answer;
2. Number of calls, offered, answered and abandoned;
3. Average Speed To Answer;
4. Average Talk Time;
5. Average Hold Time;
6. Abandon Rate;
7. Longest Wait Time;
8. Longest Talk Time;
9. Number of received and associated response times for email and web requests;
10. Categorization of ticket priority as Critical, Normal, or Low; and
11. Additional statistics based on the individual handling the contact.

C.5.6.3 TICKET CREATION

The contractor must use a standard, compliant database for storage of all tickets and supporting information. The database must support the implementation of workflows associated with:

1. Escalation of tickets (automated assignment to an organization, or generation of alerts based on logically-defined and time parameters);

2. Staff involved in the escalations and approval process must be alerted via email that an action is required within specified time frames; and
3. Support a hierarchical ticket classification scheme as specified in the contractor's SOP. Ensure all tickets that could impact Soldier pay or promotion be classified as critical.

The contractor must ensure that each ticket record contains the set of fields, which includes:

1. Type of ticket (incident, problem, and request);
2. Work log (log of steps taken in resolving the ticket);
3. Each entry must have a timestamp and ID of the person making the entry;
4. User's name, Military grade, and contact information;
5. Multi-level classification scheme;
6. Ticket Status; and
7. Assignment.

Ticket Creation Requirements: The SMMS and RCMS-G Service Desk is operated and maintained by the contractor and the contractor must provide support to the users of the SMMS and RCMS-G Suite and its products. All calls from the users are routed to the Service Desk for initial handling. To handle incoming calls, the contractor must provide live telephone coverage from 8:00 am to 8:00 pm Eastern Time- Monday through Friday, excluding Federal holidays and closures.

The contractor must:

1. Answer calls and greet the customer with a standard welcome message as provided by ARNG;
2. Verify existing or obtain new user information;
3. Identify the nature of the problem and classify it correctly;
4. Record any additional information obtained from the user;
5. Assign priority as defined by service desk operations procedures; and
6. Provide the user with a ticket number.
7. Assign unresolved tickets to a person responsible for ticket resolution

To handle emails and web submissions, the contractor must:

1. Review email and web request queues in regular intervals Monday through Friday 8:00 am to 8:00 pm Eastern Time, excluding Federal holidays. Requests that come in after close of business will be addressed starting at 8:00 am on the next business day;
2. Create tickets for each email and Web request; and
3. Contact user with ticket number.

Available statistics indicate an average call-length of seven minutes. Over a recent one year period, the call distribution was as follows and represents the number of tickets that occurred during that time period. This may or may not be similar to the actual call load, system outages and software changes may increase volume:

Time of Day of Ticket Creation	Number of Calls
8:00 am – 9:00 am	1,465
9:00 am – 10:00 am	1,548
10:00 am – 11:00 am	1,800
11:00 am – 12:00 pm	1,786

12:00 pm – 1:00 pm	1,496
1:00 pm – 2:00 pm	1,441
2:00 pm – 3:00 pm	1,387
3:00 pm – 4:00 pm	1,347
4:00 pm – 5:00 pm	998
5:00 pm – 6:00 pm	618
6:00 pm – 7:00 pm	223
7:00 pm – 8:00 pm	103
Total	14,212

Table 4 - Average Annual Service Desk Calls by Hour

C.5.6.4 MANAGING TICKETS

To manage tickets created by or assigned to the contractor, the contractor must:

1. Maintain status of all open tickets and escalate as required;
2. Coordinate resolution with other internal and external teams, as appropriate;
3. Update the users with progress of the incident resolution through the ticket and;

The contractor's staff must own the problem resolution process from the initial contact with the users to resolution of the incident regardless of whether the problem is resolved within the Service Desk or it has to be escalated to other organizations. To ensure that the users are updated with the progress of the resolution process, the contractor's staff must provide updates to the users on a daily basis. The contractor's staff must also be responsible for verifying resolutions with the users, by doing regular checks with ticket submitters of a subset of resolved tickets, to verify user concurrence in the resolution. These checks must take place on a monthly basis.

The contractor's personnel must not reject a caller based upon a problem not being within their purview. The contractor must make every effort to refer it to the most appropriate support organization. Support organizations may include external data partners, cloud help desk, ARNG IT Help Desk, or other external support organization best suited to handle the caller's issue.

Support requests that have not been closed or have not had a defect resolution identified or been put in a hold status by the government after 1 month, must be grouped if multiple users are experiencing the same or similar issues and reported to the government with an explanation of the issue and the plan to resolve the issue within 30 days. All unresolved tickets after 30 days will be reported to the government as part of an extended resolution process.

The contractor must provide an in-process review of extended resolution tickets to include a resolution POAM during each monthly technical status meeting (Reference C.5.1.2).

C.5.7 TASK 6 – SMMS and RCMS-G SYSTEMS OPERATIONS AND MAINTENANCE

The SMMS and RCMS-G systems are hosted in the ARNG Temple Jr. Army National Guard Readiness Center (TARC) in the IPN located in Arlington, VA.

The intent is for RCMS-G to be combined with SMMS and migrated into the cloud during the life of this contract. The

ARNG's desire is to host the newly combined system along with the development environment with the rest of the ARNG systems and utilize the ARNG G6 common services in a manner consistent with ECMA policies.

The systems require varying levels of upgrade to become fully compliant. Some of the current projects that are in progress and are anticipated to be at least partially completed prior to award include:

1. MS SQL Server 2012 conversion to MS SQL 2016 - SMMS
2. Application and Shared component tool upgrades from legacy Adobe Flash to modern HTML5 – Various Applications (Almost 1 Million lines of code)
3. Server consolidation and compute/store increases - System
4. Test and Development environments – prepared for a migration to an ECMA approved cloud environment with the intent to operate a full DevSecOps Software Development Lifecycle (SCDL) methodology.

C.5.7.1 SMMS and RCMS-G ENVIRONMENT

The contractor must operate SMMS and RCMS-G at the designated host facilities in accordance with the IaaS table shown in Figure 1. The IPN provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, security devices, and other common services) and manages Virtual Machine (VM) servers hosting the SMMS and RCMS-G modules.

The contractor must prepare a plan to migrate to the selected CSP Development, Testing, and Production environments. Currently only production SMMS and RCMS-G environments and a small RCMS sandbox environment are hosted in the IPN. If the test and development environments are fully migrated to the cloud they will be government provided to the contractor. The test and development environments are in a GovCloud instance. In the case that they are not available, the contractor must establish these environments on behalf of the government and will be reimbursed as an ODC by the government NTE the total ODC limit.

The Contractor must provide a cloud migration plan that includes all requirements to migrate the SMMS and RCMS-G program and identify the capabilities once the program is migrated. The Cloud Migration Plan must include all required steps and outline key milestones and dependencies for a successful cloud migration. This plan must be approved by the government prior to the cloud migration project being awarded. Cloud Migration Plan (Section F, Deliverable 54)

The contractor must prepare a plan to combine the RCMS with the SMMS. The ARNG intends to combine all services provided by these systems into a single modern environment. This includes a single sign-on and consolidated services to maximize performance. The System Consolidation Plan must include all required steps and outline key milestones and dependencies for a successful system consolidation. This plan must be approved by the government prior to the SMMS and RCMS-G system consolidation project being awarded. System Consolidation Plan (Section F, Deliverable 55)

The contractor must adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at: http://iase.disa.mil/cloud_security/Pages/index.aspx . Note: The new cyber incident reporting requirements of SRG section G.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise affect the contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this contract.

The contractor must make all reasonable attempts to schedule planned maintenance outside of peak user hours (8:00 am EST through 9:00 pm EST). When third party support is required to conduct maintenance it may not be possible to

schedule outside of these hours, however off peak hours or non-business days should be considered as ideal planned maintenance windows for scheduling purposes.

The contractor must perform maintenance necessary to respond to any Advisory, Conciliation and Arbitration Service (ACAS) scans run by host facilities.

The contractor must comply with all Army Information Assurance Vulnerability Alerts (IAVAs) in regards to upgrades and scheduling of upgrades.

The contractor will coordinate with IPN and/or CSP to schedule Full and Differential backups of VMDK files. IPN will do file level backups/restores on all VMs including VM snapshots.
The contractor must manage Development, Test, Staging, and Production environments to ensure code is promotable to production with consistent results. It is the intent of the government to host all environments in the cloud. Currently the vendor is responsible for hosting all environments other than production.

The TARC IPN provides (IaaS) support and maintains a virtualized hosting environment for the system, ensuring that the virtual infrastructure is available to the maximum extent possible. The contractor will be granted vCenter console access to view all VMware performance counters for their servers and have the ability to attach to the server console, reboot, shutdown, and turn off ARNG servers either directly or with IPN SA support.

The contractor must maintain the SMMS and RCMS-G VMs at ARNG TARC IPN through a pro Active coordination with ARNG-G6 -- staff responsible for signal/computer management.

The contractor must perform routine service and maintenance on a scheduled basis. Emergency maintenance for system operations will require support on a 24/7 basis. This maintenance must be scheduled based on a minimal user interruption plan.

The contractor must mitigate findings uploaded to the Vulnerability Management System (VMS), ensuring that all systems remain fully patched and are Army Information Assurance Vulnerability Alert (IAVA) compliant.

The contractor must ensure that all systems remain fully DISA Standard Technical Implementation Guide (STIG) compliant. The contractor must document in VMS or with a Memorandum for Record any STIG finding that cannot be mitigated stating why the finding cannot be applied and any mitigation in place to limit the vulnerability created by the STIG non-compliance.

Due to the need to comply with higher guidance from Network Enterprise Technology Command (NETCOM) and US Cyber Command the following permissions and clients will remain in effect for the system.

Domain Administrators and IMO IA personnel will remain in the local administrators groups on the servers. All personnel with access will maintain current training (IA, PII, and HIPAA) prior to being granted access.

The contractor must ensure HBSS, SCCM, and Antivirus clients are installed and functional. It cannot be assumed that ARNG IPN support staff will be available on demand. Therefore the vendor must apply a continual monitoring approach and plan for the needed assistance so that all actions can be completed on time and with minimal interruption.

The contractor is responsible for backing up SMMS and RCMS-G systems and databases to the IMO provided backup Common Internet File System (CIFS) share using either the Microsoft provided tools, or third party tools provided by the Government.

The contractor must ensure backups are not encrypted or compressed in order to maximize the efficiencies gained by using the provided backup hardware.

The contractor must monitor storage utilization and identify requirements for additional storage at least 2 weeks in advance.

The contractor must coordinate with ARNG G6 and NETCOM to provide the required web proxy and filtering.

The contractor must be responsible for ensuring annual FISMA requirements are met. These requirements include annual system security assessment, annual test of security controls, and annual testing of the system's contingency plan.

The contractor must operate SMMS and RCMS-G at the ARNG IPN hosting facility in accordance with the IaaS table shown as Figure 1. RCMS-G consists of production elements (ARNG G1 data warehouse databases, RCMS-G modules and Web server) The ARNG TARC IPN provides IaaS styled hosting environment for the physical infrastructure (racks, power, Local Area Network (LAN)/Wide Area Network (WAN), servers, firewalls, and security devices) as well as for the OS of the servers hosting the SMMS and RCMS-G modules.

The contractor must maintain the SMMS and RCMS-G test system hosted at the ARNG TARC IPN/CSP to be consistent with the production environment.

The contractor must prepare plans and execute the transition and/or integrate capabilities and data to other systems as directed by the Government while maintaining capabilities with minimal impact to users.

The contractor must maintain the SMMS and RCMS-G virtual machines at ARNG IPN environment through a pro-active coordination with ARNG-G6 to ensure operational capability and security compliance.

In the event of a situation that impacts system availability, the contractor must notify the TPOC as soon as possible after detection of the issue but not more than 12 hours after detection. Availability is measured 24/7/365 minus government approved maintenance and approved downtime outside of the contractor's control with a goal to have the system available 99.999% of the time.

C.5.7.2 WEB SERVER MAINTENANCE

The contractor must maintain operational readiness of the Web servers (currently Apache and Internet Information Services (IIS)) that host the SMMS and RCMS-G applications. There are currently five web sites hosted on the SMMS and RCMS-G server and three web sites hosted on the SMMS server. The support in this area includes:

- Ensuring web sites maintained under this contract continue to meet DoD security standards and maintain full accreditation in accordance with the security section of the PMP;
- Ensuring public web sites are registered with the most popular search engines (e.g., Google Bing, Yahoo) to increase visibility, and take actions to ensure web sites private to the SMMS and RCMS-G program are hidden from those search engines;
- Planning, coordinating, and conducting web site usability studies;
- Ensuring public web sites are registered and take actions to ensure web sites are private to the SMMS and RCMS-G program;
- Ensuring web sites, web applications, and data processes are secure and conform to the DoD Risk Management Framework;
- Planning, coordinating and conducting web site usability studies and;
- Providing a system capable of handling 6,000 concurrent visitors to the public site, conducting routine functions without system degradation.
- The contractor must provide a Web Server Maintenance Confirmation Report of completed maintenance

tickets (Section F, Deliverable 26).

C.5.7.3 INCIDENT AND PROBLEM ANALYSIS

The incident/problem resolution process involves both immediate assistance with resolving problems and analyzing issues in order to prevent the recurrence of incidents and errors. To increase efficiency of employed systems and to minimize disruption to the on-going operations of SMMS and RCMS-G, the Government is driving the SMMS and RCMS-G program toward a more proactive approach to problem management. This approach relies on the ability to correlate and analyze incidents and information from multiple sources including service desk tickets, change requests, alarms generated by automated sources and others. The goal of this approach is to identify potential problems before they actually occur and effectively improve customer service and system performance, while lowering support costs. The contractor must implement a process to actively monitor activity and identify performance. This process will allow for problem analysis and product improvement recommendations.

The support in this area includes:

- Performing analysis that leads to the identification of root cause of problems and the means of resolving them;
- Completing and submitting the root-cause analysis results, along with recommendations, to the Government for each major event (system warnings and exceptions as defined by the contractor's process), such as an event that results in an outage that cannot be resolved through standard procedure;
- Providing recommendations that are technical solutions and incorporate suggestions for improving internal processes;
- Continually performing this analysis and presenting the Government with recommendations;
- Creating and managing a database that contains information about known problems and their expected resolution that is consistent with Information Technology Infrastructure Library's (ITIL®) Known Error Database approach and;

The contractor must present the summary results of the analysis, along with recommendations for improvement, as a part of the Monthly Status Report (Reference C.5.1.3). The contractor must provide an Incident and Problem Analysis Confirmation Report of Completed Tickets (Section F, Deliverable 27) Approximately 10,000 help tickets per year are expected.

C.5.7.4 ENGINEERING SUPPORT

The contractor must provide engineering support to meet the changing needs of the SMMS and RCMS-G user community, maintain industry best practices, and plan for long-term growth and sustainability of the SMMS and RCMS-G Suite. The contractor must identify potential projects to improve SMMS and RCMS-G capabilities and engineering changes needed to meet program objectives. The contractor must perform additional engineering initiatives, to support changing technologies or are based on emerging requirements identified by the ARNG.

Engineering support must include:

1. Providing technical improvement recommendations to ongoing SMMS and RCMS-G O&M efforts;
2. Anticipating changes in the SMMS and RCMS-G technical and business requirements and making recommendations implementing industry best practices;
3. Providing technical and business recommendations to support the SMMS and RCMS-G strategic planning process;
4. Assessing impact of changes to SMMS and RCMS-G requirements on technical and cost baselines;
5. Any changes or engineering support that become a requirement by a change in law, regulation, or policy that are not covered in the scope of this contract must be; coordinated through the COR/CO for approval and contract modification
6. Providing ongoing coordination with software maintenance team(s) for tailored products, modules and models database and best practices support as provided by users to make engineering revisions;

7. Preparing, planning, and migrating hosting of the SMMS and RCMS-G Development, Testing, and Production environments to a FEDRAMP approved DoD Cloud Service Provider (CSP) as directed by the government and;
8. Migrating capabilities into a common solution that provides a low code data driven software solution focused on providing support to all types of software maintenance
    a. Adaptive Maintenance
    b. Perfective Maintenance
    c. Corrective Maintenance
    d. Preventative Maintenance.

C.5.7.5 DEVELOP OPERATING LEVEL AGREEMENTS

Working with other ARNG support contractors: ARNG employs the services of multiple contractors and Vendors in support of its operations (approx. 50).

The contractor must work with these entities and establish working agreements (e.g., OLAs) as needed to provide support that meets the requirements under this PWS.

ARNG will assist with coordinating the interactions between the SMMS and RCMS-G contractor and the other support contractors as needed.

C.5.7.6 CHANGE IMPLEMENTATION

The SMMS and RCMS-G is constantly changing and expanding. This expansion is primarily driven by: (a) availability of new data elements, (b) user requests, (c) technology evolution, and (d) ARNG mandates.

To support this expansion and changes, the contractor must:

1. Provide technical resources and capabilities to change existing and implement new business logic and to update and change the SMMS and RCMS-G environment and its offerings;
2. Create and verify fields and metrics; and
3. Create new metrics (metadata and equations) to support new features, add new data sources or data versions, and make changes to SMMS and RCMS-G products.

The contractor must be responsible for delivering the Configuration Management Plan within 30 days of TO award (Section F, Deliverable 33). The contractor must demonstrate a working

Configuration Management Database within 60 days of TO award (Section F, Deliverable 34). The contractor must take precautions while engineering changes.

Document dependencies as they become known;

1. Create test scripts to test all changes. Test scripts may be manual or automated;
2. Exercise test scripts for all major components after any system deployment;
3. Use a Training Application for all tests before deployment to Production Application;
4. Create system rollback points prior to implementing new changes;
5. Advise the Government within 24 hours of a self-inflicted error and document the dependency to avoid future instances of creating the same error;
6. Change work must not begin without COR/TPOC concurrence;
7. Change SMMS and RCMS-G functionality as mandated by DoD, Active Component, and ARNG manpower and human resource management policy changes;
8. All changes must follow the change management process. These solutions require implementation of good software change practices;

9. Implement dual directional data interfaces between SMMS and RCMS-G and Integrated Personnel and Pay System Army (IPPS-A). Support data calls and testing of interface to IPPS-A system to ensure that the required system interfaces between SMMS and RCMS-G and IPPS-A provides accurate incoming and outgoing requirements; and
10. Modify and optimize the SMMS and RCMS-G product, module, and model suite: Modify and optimize the SMMS and RCMS-G Suite to integrate with new operating systems, compilers, system utilities, and other system products as well as operate the Configuration Management process throughout the contract to include identification and labeling of configurable items, maintenance of configurable items, configuration verification and auditing with records auditable over time.

C.5.7.7 CONFIGURATION IMPLEMENTATION

An approved Change Request (CR) enters the Change Implementation process. The contractor must implement changes to the system as identified in the Change Management process. To support Change Implementation the contractor must:

1. Add, modify and delete code and business logic to implement changes;
2. Add, modify and delete data metrics in the data warehouse;
3. Add, modify and delete source code from a repository with branches dedicated branches for testing, development and production code;
4. Modify the system environment as required to implement change (inclusive of adding, modifying or deleting external data feeds);
5. Create test scripts for user acceptance testing;
6. Conduct user acceptance testing, regression testing, unit testing and other types of testing as required to implement the change;
7. Update system documentation after changes are implemented;
8. Summarize system changes completed on the Monthly Status Report (Reference Section C.5.1.2).
9. Maintain and change the SMMS and RCMS-G test strategy that includes unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach. This strategy identifies data or software issues which, if not resolved, may threaten accuracy and operational status of SMMS and RCMS-G;
10. Develop and use System/Software Testing Checklists as outlined by the Software Test Plan to document testing of changes, or new developments. Testing must include unit, integration, system, and acceptance testing from both a top-down and a bottom-up approach;
11. Test all changes prior to implementation to prevent the occurrence of any potential problems in products, modules, models, or systems and;
12. Maintain and report testing artifacts, including defect type, status, and resolution.

The ARNG will define specific change efforts based on information brought forward by internal and external stakeholders.

C.5.7.8 COOP SUPPORT

The contractor is responsible for and must perform standard backups and software/data copies that support the ARNG providing and managing the COOP environment and equipment. To include troubleshooting and SMMS and RCMS-G specific SME support to the ARNG G6. The contractor must provide an assessment of the existing COOP that identifies the existing process and potential weakness that the government should address. This plan must be continually updated as the COOP procedures change or the environment changes (i.e. Cloud Migration) (Section F, Deliverable 29).

C.5.7.9 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology (IT) accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or

use electronic and information technology.

All electronic and information technology (EIT) procured through this task order must meet the applicable accessibility standards specified in 36 C.F.R. § 1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this task order are listed below.

The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport, and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment.

Applicable Standards, which apply to this acquisition:

Section 1194.21: Software Applications and Operating Systems____X_____.
Section 1194.22: Web-based Internet Information and Applications____X_____.
Section 1194.23: Telecommunications Products_____.
Section 1194.25: Self-Contained, Closed Products_____.
Section 1194.26: Desktop and Portable Computers_____.
Section 1194.31: Functional Performance Criteria_____.

C.5.7.10 PROVIDE SMMS and RCMS-G TECHNICAL INFRASTRUCTURE LIAISON SUPPORT

The contractor must provide dedicated and direct technical support to the ARNG IPN to plan and improve network and infrastructure posture. This will require individuals to have elevated system access and therefore an IAT II or higher qualification is required.

The dedicated IPN technical contractor must provide support to:

1. Troubleshooting and repairing IAVA installation
2. Installing and troubleshooting security software (McAfee Products)
3. Troubleshooting and repairing backup access and replication activities
4. Performing required security scans
5. Security Technical Implementation Guide (STIG) management
6. Supporting internal CAB and other approval boards
7. Support to CCRI and ATO activities within the ARNG IPN
8. Provide general troubleshooting and repair of network and system level support to ensure system and network compliance

C.5.7.11 BUSINESS PROCESS DOCUMENTATION

The Contractor must manage the development of solution-specific architecture viewpoints; create and maintain DoD Architecture Framework (DoDAF) architecture viewpoints to ensure the architecture remains consistent with current solution configurations and designs; and ensure compliance with the prevailing release of the DoD Business Enterprise Architecture (BEA).

C.5.8 TASK 7 – APPLICATION AND FUNCTIONAL SUPPORT

The contractor must identify and respond to defects or faults in the SMMS and RCMS-G Suite of applications, modules, performance or function. The contractor can expect approximately 320 corrective maintenance activities per year. Many application layer change requests can be completed by functional subject matter experts through metadata

updates utilizing the existing low code environment, thus requiring less involvement from traditional software developers.

The support in this area includes:

- Producing and implementing a process to identify, track and resolve defects. This process must include the development, test, and production environments with identification by Quality Control Testers, Metadata managers, and/or Software developers, as well as field users;
- Defining a process to address high impact defects as well as routine defects;
- Ensuring that web applications are scalable to meet the future needs of the ARNG, and that applications make maximum practical use of object oriented design and component reusability;
- Ensuring requirements for all SMMS and RCMS-G modules and applications are met;
- Tracking all defects as service desk tickets and updates information about their status and resolution;
- Providing the capability to identify and respond to inquiries of data abnormalities contained within SMMS and RCMS-G data source as it relates to historical data sources. Responses are required within 12 hours and;
- Providing the capability to inform Users when any module or application is offline or down for Maintenance or updates.

The contractor must provide a Defect Identification, Tracking and Resolution report, (Section F, Deliverable 53).

C.5.8.1 STANDARD REPORT GENERATION AND DISSEMINATION

The contractor must ensure that all standard reports are generated, verified, and delivered to the recipients in a prearranged manner. Standard reports are recurring reports with the same data elements with format provided by the government (Section F, Deliverable 30). The majority of reports are available either as fixed reports or user-defined ad-hoc reports, however some reports are standard and recurring, but are not available through an automated process and should be reviewed for potential automation within the RCMS-G Module Director's Personnel Readiness Overview (DPRO.)

The contractor must:

1. Use statistical sampling methods to verify accuracy of the reports;
2. Ensure that all reports and data files have been delivered by the agreed upon date and time;
3. Ensure that all pre-scheduled reports have run and can be accessed;
4. Ensure correctness of the reports in terms of format and integrity of data;
5. Create raw data sets, using either manual or automated process, for delivery to recipients.
6. The contractor must update standard reports monthly and upon request. All monthly reports are due NLT the 10th calendar day of each month (if the 10th falls on a weekend/federal holiday, the report is due the last business day prior to the weekend/federal holiday). Complex data requests requiring the assistance of technical support will be initiated within 24 hours of receipt, and timelines for completion must be maintained in accordance with the timelines developed during the change management process.

All reports must be completed/packaged according to the corresponding formats provided by ARNG, Office of the Under Secretary of Defense Personnel and Readiness (OUSD (P&R)), Deputy Chief of Staff, G1 (DAPE-MP), regulatory and statutory guidance. At any time, OUSD (P&R) or DAPE-MP can change the format, reporting dates, or add or delete reports.

C.5.8.2 AD HOC QUERIES AND REPORTS

The Government requires ad hoc queries and reports to be created each month. The tables below provide data on the number and structure of these queries and reports. The contractor is expected to produce 100-150 ad hoc queries per month (Section F, Deliverable, 31). Each Ad Hoc Report must be tested and verified before providing the report to the Government. The information shown is based on historical data; the size and structure of the queries and reports may

vary in the future. Ad hoc reports are custom reports that cannot typically be created using the DPRO application, however can lead to new DPRO reports or data metric creation that can be added to an established or new data-mart for consumption in the DPRO application. Many Ad hoc queries require an analyst that is an experienced user of Microsoft Excel, Power Point, and Microsoft SQL Server Management Studio. Data can be pulled from external and/or internal sources such as the SMMS and RCMS-G G1 Data warehouse to respond to an ad-hoc request. This support is typically embedded with the government data support team at the government site.

Table 1 - Type of Effort Required for Ad Hoc Queries and Reports

Type of Effort	Work Load (for Experienced SMMS and RCMS-G SQL Analyst)
Small	< 4 hours
Medium	4-24 hours
Large	> 24 Hours

Table 2 - Level of Effort Required for Ad Hoc Queries and Reports

Priority of Effort	Response Time
High	Less than 4 hour turn around (estimated 80-100 per month)
Medium	24 hour turn around (estimated 15-35 per month)
Low	96 hour turn around (estimated 5-15 per month)

C.5.8.3 CHANGE AND CONFIGURATION MANAGEMENT SUPPORT

Change Management focuses on how any change in the system is determined. The change management system incorporates activities such as identification of changes, impact analysis of changes, documentation of CRs, Change Control Boards (CCB), communications to stakeholders, and implementations of approved CRs. All CRs require the TPOC's signature prior to entering the Change Implementation process. The Change Control Board is a government led, contractor facilitated board that focuses on change management and scheduling.

Configuration Management focuses on how any change to the system must be performed. The Configuration Management Database (CMDB) is central to the process of Configuration Management. The CMDB includes information about the system's hardware and software as well as relationships between assets. The CMDB displays this information over time and can be used for activities such as root cause analysis, impact analysis, and Change Management.

C.5.8.3.1 CHANGE MANAGEMENT

The contractor must be responsible for delivering the Change Management Plan within 30 days of time of TO award (Section F, Deliverable 32). The contractor must operate the Change Management process throughout the contract to include Change Request collaboration and facilitation of the Change Control Board. The Contractor must plan and conduct approved software releases at least once monthly, and metadata updates at least weekly.

The SMMS and RCMS-G has three levels of changes to the application as described below:

Type of CR	Change Criteria	Estimated Number of Changes Annually
Minor Change Request (MCR)	Minor impact on requirements with no impact on infrastructure or environment 5 Business Days to develop change management documentation and initial estimate (e.g., change in icon color, changing metric)	1,950
System Change Request (SCR)	Minor to moderate impact on requirements with no impact on infrastructure or environment 15 Business Days to develop change management documentation and initial estimate (e.g., product changes, new report capability)	175
Engineering Change Proposal (ECP)	Minor to major impact on requirements and may impact infrastructure or environment. 30 Business Days to develop change management documentation initial estimate (e.g., major system changes)	6

Table 3 - Type and Frequency of CRs

The contractor must maintain a list of all applications in the SMMS and RCMS-G suite in the Application Owner Report (Section F, Deliverable 50). The contractor must review all CRs and create an initial estimated CR classification. CRs that are determined to be a MCR must be approved by the application owner. CRs that are determined to be an SCR or ECP must be approved at the CCB. Once the contractor has received approval for the SCR/ECP, the contractor must provide the government a work hour estimate that will be presented to the government.

The government will determine if the Change Request Estimate (Section F, Deliverable 52) is complete and accurate and will accept or deny the estimate. Once the estimate is approved, the work will be scheduled for a release. All approved change requests (MCR/SCR/ECP) will be scheduled during the CCB. The contractor must develop and update the Integrated Master Release Schedule (IRMS) (Section F, Deliverable 51). The contractor must report as part of the IMRS the number and category of releases made each contract year and the cumulative over the life of the contract.

Emergency CRs must be presented within 12 hours of contractor notification. The type of CR must be determined and, if required, an estimate must be completed NLT the following business day. All emergency CRs will be reviewed during the weekly CCB to determine if the IMRS will need to be modified to accommodate the emergency change. If the work is so urgent that it must be addressed prior to the next scheduled CCB, then a special emergency CCB will be conducted to address only the emergency CR and determine if a special release or patch must occur prior to the next scheduled release.

C.5.8.4 ANALYTICAL SUPPORT

The contractor must provide analytical support for analysis of issues related to achieving and maintaining personnel readiness objectives and ad hoc responses to a wide range of complex questions raised by external and internal organizations.

The contractor must make recommendations to the Government to most effectively integrate the diverse sources of data in SMMS and RCMS-G and to categorize/define the issues and problems that meet ARNG policy needs.

The contractor must provide a limited number of personnel supporting analytics functions. The contractor assigned analysts must:

- Apply objective, analytical, and orderly thinking to the analysis of complex operational and management problems, and supporting this analysis when appropriate with the use of tools and techniques such as statistical inference, models, mathematical programming, and simulations
- Conduct studies, research and prepare reports for executive level presentation
- Address specific data extraction and manipulation requirements including the ability to extract data from the G1 Data warehouse utilizing MS SQL Server Management Studio
- Identifying and formulating solutions to problems ranging from minor data quality issues to strategic forecasting of future personnel trends
- Conducting qualitative and quantitative analyses of complex military personnel and readiness issues
- Summarizing and synthesizing complex analyses into simplified terms for presentation to decision makers
- Integrating techniques into operational processes and algorithms used in the daily data preparation and quality control of the data warehouse
- Conduct Metadata analysis and modify metrics and workflows to establish greater accuracy and more automated functions.
- Provide results in a Monthly Ad Hoc report, (Section F, Deliverable 36)

C.5.8.5 PROVIDE SMMS and RCMS-G PRODUCT LEAD SUPPORT

The contractor must designate Product Leads (PLs)for each SMMS and RCMS-G product, module, model, and prototype to interface with the ARNG POCs and user community. Each SMMS and RCMS-G liaison may handle multiple SMMS and RCMS-G products. Support personnel must possess the ability to manage and define metadata, extract application specific data utilizing MS SQL Server Management Studio, and provide regulatory and policy expertise to support the projects and applications in which they are supporting.

Contractor Product Leads must be responsible for:

1. Working with ARNG POCs to determine, recommend, prioritize and verify implementation of adaptation, maintenance, and change efforts;
2. Maintain continuous communication with ARNG POCs for program policy and implementation of the SMMS and RCMS-G products, modules, and models;
3. Convey requirements between government module functional owners and the contractor's program management team, create change requests, support advanced ad-hoc SQL data requests for their products; and
4. Assist government functional module owners with the change management process.

Organizations Supported
Strength Maintenance (HRR)
Operations (HRM)
Personnel Systems (HRP)
Personnel Policy (HRH)
Resources (HRZ-RI)
Human Capital Management (HCM)
Information Systems (HRI)

Table 5 - Product Lead Support

C.5.8.6 SMMS and RCMS-G SYSTEMS MAINTENANCE

The contractor must maintain each of the SMMS and RCMS-G modules to ensure that they perform in accordance with the specified functional and performance characteristics as defined in the documentation for each module.

The contractor must:

1. Ensure the capability to upload, store and make edits to program policies;
2. Provide the capacities to view the definition of any code by hovering over the code with the mouse clicker;
3. Use common lookup tables where possible to minimize the number of locations requiring updates, update all lookup tables to conform to current policy and regulation. Lookup tables that are guided by regulation (MOS changes, and data codes standardized across the Army or DoD) must be updated within five business days of the regulation change and must take effect on the effective date of the regulation change;
4. Ensure access requests and approved use DD Form 2875 thru the User Management tool.
5. Add, Modify, and archive work flows to ensure system functions are compliant with current ARNG business functions.
6. Ensure the DD Form 2875 is updated annually and
7. Add, modify and archive database metrics

C.5.9 TASK 8 – CLOUD MIGRATION SUPPORT (OPTIONAL)

Cloud migration as a task is a single service. The contractor must develop and execute a plan to transfer hosting of the system to a DOD Cloud Service Provider (CSP) upon notification from the Government.

Neither SMMS nor RCMS-G is currently on a production cloud environment but both are in the process of evaluating hosting environments for an eventual move. The contractor must be prepared to conduct the migration of all SMMS and RCMS-G production and non-production environments to a ECMA approved CSP.

Regardless of system location and status under each phase, the contractor must achieve four goals for each configuration. These goals include:

1. Complete cyber security requirements;
2. Configure modules, applications and system artifacts for operation;
3. Ensure internal and external data feeds and data processing continue on schedule; and
4. Operate a functional and complete backup and Disaster Recovery plan.

The contractor must adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time of contract award) found at

http://iase.disa.mil/cloud_security/Pages/index.aspx (Note: the new cyber incident reporting requirements of SRG section F.4 become enforceable by the Government upon the effective date of the information collection governing the new reporting requirements (see DFARS case 2013-D018). However, this does not abrogate, limit, or otherwise affect the contractor's obligation to comply with any other cyber incident reporting or other reporting requirement that is contained in this contract).

The contractor must comply with, and enforce IA Workforce standards/ IAT Levels of baseline certifications for the Cybersecurity workforce to include computer environment certifications as applicable.

The contractor must deliver to the Government or any successor contractor, all system data, to include all code, software, and tools necessary to maintain the cloud hosted environments without interruption upon the conclusion of performance or at the request of the government.

The contractor will also be responsible to:

- Deliver a final migration plan and POAM for the total migration of all environments to the selected CSP within 30 days after the government exercises the optional CLIN
- Perform code scans as outlined in Task 3 to ensure code and data moved to the cloud environment is compliant with CSP and cloud environment standards and comply with Application Security Development (ASD) STIG;
- Evaluate SMMS and RCMS-G to ensure it will be supported in the designated cloud environment;
- Modify SMMS and RCMS-G as necessary to transition to the designated cloud environment;
- Implement all applicable security controls with a continuous monitoring plan IAW National Institute of Standards and Technology (NIST) Risk Management Framework and DoD standards;
- Maintain logically segregated development, testing, and production environments/enclaves;
- Provide hosting and backup services for Web, Mobile and IVR platforms. Service will include, as required by RMF, a secondary, redundant, independent infrastructure for emergencies/business continuity purposes; and
- Maintain the CSP environment in accordance with the DoD Risk Management Framework (RMF).

The contractor must provide the Government with cybersecurity materials, e.g. system security scans, configurations, proof of certification for system administrators, Federal Information Security Modernization Act of 2014, and DoD cybersecurity compliance information and artifacts as required under RMF within five business days of written request from the Government. The information must be included in the Cloud Migration Report (Section F, Deliverable 24).

C.5.10 TASK 9 – SMMS and RCMS-G DATA WAREHOUSE CONSOLIDATION (OPTIONAL)

The SMMS and RCMS-G Data Warehouse is currently a mix of application specific databases (Transactions) and data imported into SMMS and RCMS-G from external sources. Some data procedures exist in RCMS and replicate data into the SMMS Data Warehouse, while others exist in SMMS and replicate data into the RCMS Data Warehouse. The government intends on combining these procedures into a single data warehouse with optimal and streamlined procedures that limit processing and replication. This task may be completed independently or as part of task 10 or task 14.

The contractor will also be responsible to:

- Deliver a final consolidation plan and detailed POAM for the total integration and consolidation of all data and database procedures currently hosted on two separate DB servers SMMS and RCMS-G) within 30 days after the government awards the optional CLIN
- Complete the consolidation effectively and efficiently no later than 12 months after award of the optional CLIN.

- Provide innovative solutions and upgrades that results in gained efficiencies and lower cost of ownership for the ARNG.
- Establish current data feeds in the new environment.
- Update documentation such as data processing guide, data dictionary, ISA, MOUs, ATO, and SORN.
- Ensure the same or greater level of Cybersecurity and compliance, adhering to the standards of the legacy systems which are outlined in Task 4 (3.5.4) Cybersecurity and Compliance.
- Minimize disruption to ARNG operations by ensuring system availability.
- Provide updated Enterprise Architecture diagrams and documentation (Complete RMF update)
- Maintain the standards set forth in section C.5.2 and C.5.3

Output: The contractor must provide an in process review in the Monthly Status Report – Data Warehouse Consolidation (Reference C.5.1.2)

C.5.11 TASK 10 – SMMS and RCMS-G SYSTEM CONSOLIDATION (OPTIONAL)

The contractor will provide a consolidated system solution for SMMS and RCMS-G. The contractor must:

- Deliver a POAM for the total integration and consolidation of the suite of modules/applications currently hosted on the two separate systems (SMMS and RCMS-G) within 30 days after the government awards the optional CLIN
- Complete the consolidation effectively and efficiently no later than four months after award of the optional CLIN.
- Provide innovative solutions and upgrades that results in gained efficiencies and lower cost of ownership for the ARNG.
- Provide a single URL and single sign-on for accessing all SMMS and RCMS-G modules.
    - Utilize the Enterprise Access Management Service-Army (EAMS-A) for user authentication. EAMS-A manages access to secure Army sites by verifying a user's identity and permissions. All personnel issued a Common Access Card (CAC) are automatically provisioned in the EAMS-A enterprise directory. Certain SMMS modules may require a separate URL and sign-on such as self service portals.
- Establish current data feeds in the new environment.
- Update documentation such as data processing guide, data dictionary, ISA, MOUs, ATO, and SORN.
- Update system registrations such as e-MASS, APMS, Whitelist, and DNS.
- Ensure the same or greater level of Cybersecurity and compliance, adhering to the standards of the legacy systems which are outlined in Task 3 (3.5.3) Cybersecurity and Compliance.
- Redirect the RCMS URL to the new location
- Minimize disruption to ARNG operations by ensuring system availability.
- Provide updated Enterprise Architecture diagrams and documentation (Complete RMF update)

Output: The contractor must provide an in process review in the Monthly Status Report - System Consolidation (Reference C.5.1.2)

C.5.12 TASK 11 – SMMS and RCMS-G COOP (OPTIONAL)

SMMS and RCMS-G COOP policies fall under the general COOP policies and procedures in use by the hosting center. The contractor must ensure that all COOP activities are scheduled and completed. In general, any updates to the production systems are automatically replicated to the COOP site. The COOP site for SMMS and RCMS-G is procured and hosted by the Government and the Government purchases all hardware and software needed to maintain the alternate COOP site. Under this contract, the contractor must ensure that all the equipment at the alternate COOP site is configured identically to the maintained equipment at the locations that support the primary SMMS and RCMS-G environment. The contractor must verify that every change to the production environment is reflected in the COOP environment within 24 hours.

The contractor must test the COOP and disaster recovery systems and operational plan at least quarterly during the

Base Period of the contract and during each Option Period of the contract.

During a state of emergency, the contractor must supply essential personnel as identified in the Information System Contingency Plan (ISCP); The SMMS and RCMS-G ISCP establishes comprehensive procedures to recover SMMS and RCMS-G quickly and effectively following a service disruption. Essential personnel are identified as contract support personnel in support of the ISCP. Depending on the type/level of crisis, these personnel will begin communication immediately with the SMMS and RCMS-G System Owner to ensure recovery and operations of the system in accordance with the ISCP.

The contractor must ensure that all systems within the alternate COOP facility are ready to take over operations from the systems located at the primary location for SMMS and RCMS-G environment within Recovery Time Objective (RTO) and Recovery Point Objective (RPO) limits after primary system's failure. This requires the contractor to ensure that the alternate COOP systems:

1. Recovery Time Objective (RTO) is 4 hours. Recovery Point Objective (RPO) is 724 hours;
2. Have the same software release levels and patches as the primary SMMS and RCMS-G systems;
3. Are configured with the same configuration information as the primary systems; and
4. Are capable of operating on their own in case of partial or complete failure of the primary systems.

The contractor must (in coordination with the government) develop and maintain a COOP and ensure the COOP Plan is coordinated with the TPOC and ARNG G6 in order to ensure system operation in the event primary system infrastructure becomes inaccessible. This task is enhancing the existing COOP capabilities in TASK 6, and will result in fast cut over/ redirect "Hot COOP" that greatly reduces required down time in the event of an unplanned COOP event.

The contractor must:

- Evaluate the technologies and services available at hosting environments to determine the most cost effective means to meet RTO and RPO limits;
- Review and provide recommendations to the government on changes to COOP and Disaster Recovery to the Government on an annual basis. Recommendations will include technical details, costs, and RTO/RPO projections;
- Identify and report to the government the resources required to implement COOP operations;
- Supply essential personnel as identified in the Information System Contingency Plan (ISCP) in support of a state of emergency;
- Maintain a COOP that is coordinated with the ARNG G6 in order to ensure that all systems will be operational during any of the events that will trigger a COOP operation;
- Maintain the environment and applications at production and COOP locations;
- Verify that every change to the production environment is reflected in the COOP environment within 48 hours of final user acceptance;
- Ensure that all the equipment at the alternate COOP site is configured identically to the maintained equipment at the locations that support the primary SMMS and RCMS-G systems; and
- Ensure the SMMS and RCMS-G systems' pre-production and production environments are documented in build guides so that the environments and systems can be rebuilt as necessary.
- Maintain up to date data at the COOP location to ensure all COOP events match the most recent data processing

The contractor is required to be readily available in performance of this task upon Optional CLIN award.

Output: The contractor must provide a COOP Implementation Report (Section F, Deliverable 28) 30 days from Optional CLIN award

Output: The contractor must provide an in process review in the Monthly Status Report - COOP (Reference C.5.1.1)

.

C.5.13 TASK 12 – HISTORICAL DATA REPROCESSING (OPTIONAL)

Data reprocessing occurs frequently under Task 2 (3.5.2) as a small percentage of data from external sources is observed to have corruptions that were not identified during data quality checks applied prior to insertion into the data warehouse. However, periodic data checks and service desk inquiries will reveal additional data anomalies, with some requiring historical data reprocessing to resolve. This task intends to combine all significant data quality issues and reprocess all data required to remedy the inaccuracies. In many cases this will require the data to be rerun from the date of the incident through the current date and then all dependent tables to be rerun to account for these updates.

The contractor must:

- Analyze all data warehouse data to identify data anomalies and from service desk tickets or SMMS and RCMS-G functional experts for their overall impact to the system and to the ARNG and its service members.
- Create a service ticket for each data anomaly discovered that is not already documented in the ticketing system. For all anomalies assessed with a moderate or higher overall impact to the system, the ticket will outline the steps required to reprocess the data, to include a level of effort and provide a SQL script that clearly demonstrates the anomaly.
- Finalize the consolidated Historical Data Reprocessing Plan and obtain government acceptance. The plan must include all required steps and outline key milestones and dependencies for a successful data reprocessing to include a mitigation plan that minimizes the disruption to users. Within 30 days of award of Optional CLIN;
- Execute the Historical Data Reprocessing Plan as approved to reprocess historical data in the same manner as 3.5.2. In some cases, the volume of data required to be reprocessed may span multiple weeks, months, or even years, depending on the severity of the anomaly.
- Document the improved data quality by providing the government the initial SQL output and analysis that identified the anomaly and the post historical reprocessing results. To include the SQL Scripts that generated the data.

The Contractor must provide a complete list of all historical data anomalies with a cumulative level of effort to reprocess each data point (i.e. some issue may not require any additional time to repair if it occurs multiple times, as the DBA would start from the earliest occurrence and update all data through current). The vendor must develop a reprocessing plan that incorporates as many quality improvements with the minimal amount of effort. This planning must include updating all dependent tables. It is estimated that several tables have multiple occurrences of data anomalies that occurred in various months dating back to at least March 1, 2016 that impacts hundreds of total data points. This data reprocessing effort requires a technical database administrator to utilize the SMMS and RCMS-G Data Processing Guide (DPG) and since this is a data warehouse cannot be done solely by replacing independent tables. As identified in Section C.5.2 this will require a combination of SQL and mainframe tasks.

The Contractor must provide a Historical data Re-processing report (Section F, Deliverable 47) as part of the MSR (Reference C.5.1.1).

C.5.14 TASK 13 – METADATA TRAINING (OPTIONAL)

The SMMS and RCMS-G Suite of applications utilizes a low code data driven architecture that is reliant on metadata to make many system updates to include UI, WorkFlow, and metric changes. It is the Government's intent to certify select users as expert users and allow control of metadata to be a shared service.

The contractor must develop a training program to allow for the training and certification of select government employees to make these edits. The contractor must develop an introductory, intermediate, and advanced SMMS and RCMS-G metadata course that provides all the documentation and knowledge to successfully perform these tasks.

The course must consist of practical exercises and examinations that certify the government employee as qualified to perform the functions taught.

The contractor must conduct at least two training sessions per training level at the contractor location or virtually if

approved by the government annually. Training sessions should take approximately five days to cover all relevant material and complete the practical exercises before completing the end of course test. Training can be held in consecutive or independent sessions, and all three levels must be passed prior to the government being granted access. The trainer must be fully certified and an industry expert in the SMMS and RCMS-G metadata.

Specific Course Material must include:

- A training version of the software that is dedicated to classroom instruction
- Relevant training material that addresses actual Army programs (either Current or Historical)
- Intermediate and advanced training must have practical exercises that must be completed as a prerequisite prior to starting in person training. These prerequisites must be available as independent study opportunities.

The contractor will also be responsible to:

- Only certifying government employees that pass relevant exams with at least a 90%;
- Make available access to the metadata and state machine editor tools to individuals who become qualified;
- Provide training in a fixed format that is repeatable with all necessary training materials;
- Include government modified metadata into test packages prior to release so that all changes are verified and tested prior to release ;
- Ensure the training courses are portable so that the government and other parties can conduct training in the future;
- Ensure no course is longer than one week in duration; and
- Maintain the courses as software updates occur to ensure training is kept up to date

The contractor must provide an in process review in the Monthly Status Report - System Consolidation (Reference C.5.1.2)

C.5.15 TASK 14 – IPPS-A CONVERSION (OPTIONAL)

The Integrated Personnel Pay System – Army is a new Army Enterprise Resource Planning (ERP) that is currently being used for all three Army Components. The ARNG currently receives personnel data in two ways. This task may be completed independently or as part of task 9 or task 10.

1. From IPPS-A through an inbound data feed that is in a format similar to the legacy SIDPERS application.
2. From Total Army Personnel Database – Guard (TAPDB-G)

When IPPS-A Release 3 is deployed it will implement a large-scale data dictionary change and TAPDB-G will sunset. SMMS and RCMS-G will need to do a complete review and remap of all data metrics to ensure data integrity and accuracy. It is anticipated that SMMS and RCMS-G will subscribe to the IPPS-A system to pull data rather than continue to rely on an antiquated data push from IPPS-A. Due to the nature of a data subscription this will allow SMMS and RCMS-G to pull near real-time information. It is ARNG's intent to pursue all data updates no more than 24 hours in advance for all personnel data. This change will require a change to most stored procedures that load and process data in addition to the potential for adding additional data and consolidating many legacy processes.

The contractor will also be responsible to:

- Map all data elements of IPPS-A to the existing data point in SMMS and RCMS-G and create a mismatch report;
- Create a data migration plan that will remap all data IAW the new data standards;
- Streamline and consolidate database procedures to optimize data processing;
- Create special quality reports for ARNG data that originates in IPPS-A (This is currently a TAPDB-G function);
- Create optimized jobs that pull the IPPS-A data into SMMS and RCMS-G efficiently;
- Ensure SMMS and RCMS-G data quality remains at least as high as it is now;
- Limit system interruption of SMMS and RCMS-G users;
- Coordinate directly with IPPS-A technical data experts to improve all database processes and procedures;

- Review all existing data quality checks, indexes, and overall data warehouse performance to ensure for optimal results; and
- Conduct a review of Data Operation SLA's to reduce the amount of time allowed for data processing.
- Update all system documentation IAW Task 2 and all applicable RMF standards;
- Update all procedures and documentation in the DPG

The contractor must provide an in process review in the Monthly Status Report - System Consolidation (Reference C.5.1.1)

The contractor must conform to at least the standards set forth in section C.2 Data Processing Status ReportOutput: IPPS-A Conversion Status Report (Section F, Deliverable 48)

C.5.16 TASK 15 –MAINFRAME CONVERSION (OPTIONAL)

SMMS and RCMS-G currently rely on the Army Mainframe located at the Joint Service Provider in the Pentagon. As described in the DPG, several data processing tasks rely on key data and functions performed on the Mainframe. This is inclusive of the millions of individual soldier pay records from DJMS AC/RC.

The Mainframe equipment is reaching end of life and is not anticipated to be replaced. This processing and the subsequent data feed must be updated to be performed with the rest of data processing in MS SQL server. This task may be completed independently or as part of task 14, task 9, or task 10.

The contractor will also be responsible to:

- Provide the Government with a detailed explanation and requirements for the additional compute and store needed to perform these tasks in SQL;
- Convert all Mainframe processes to SQL server jobs and procedures;
- Coordinate the required system interface changes;
- Create the ability to store this data in SQL to include backups similar to the Mainframe;
- Update the DPG with the new procedures;
- Test and ensure accuracy of all new and existing data;
- Limit system interruption of SMMS and RCMS-G users;
- Update all system documentation IAW Task 2 and all applicable RMF standards;
- Review all existing data quality checks, indexes, and overall data warehouse performance to ensure for optimal results; and
- Provide a decommission plan and upon government approval decommission the ARNG Mainframe.
- Update ISA

The contractor must provide an in process review in the Monthly Status Report – Mainframe Conversion Report (Reference C.5.1.1)

The contractor must conform to at least the standards set forth in section C.2 Data Processing Status Report Mainframe Conversion Status Report (Section F, Deliverable 49)

C.5.17 TASK 16 –ARMY INCENTIVE MANAGEMENT SYSTEM (AIMS) INTEGRATION (OPTIONAL)

U**SING** the ARNG Guard Incentive Management System (GIMS) and/or the USAR's Reserve Incentive Management System (RIMS) software with configuration of the Active Army's data sources, business rules and processes, a more definitive framework can be leveraged to provide for stronger management controls for Bonus and Incentive contracts and payments in accordance with law, DoDI, Army Regulation, and policies. This framework must include an automated approach for contracts and payments that ensures more efficient, expedient, and accurate processing. Establishing visibility across the full lifecycle of contracts and payments will create an increased awareness and accountability. It can also help achieve the following objectives:

- Utilize existing systems and records to populate the Management Center Module with historical and current incentive contracts.
- Utilize existing legislation, regulations, policies, systems and records to populate the Administration Center Module with business rules.
- Utilize existing legislation, regulations, policies, systems and records to populate the Information Center Module with applicable documentation.
- Utilize current allocations and Program Objective Memorandum (POM) projections to populate the Plans and Strategy Center Module with current and out-year budgets.
- Utilize existing systems and known stakeholder information to populate the User Management Tool (UMT) Module.
- Utilize existing system and manual reports to populate "canned" reports in the Reporting Center Module.
- Identify active System Interface Agreements (SIAs) for existing systems, as well as, identify and create additional, applicable SIAs.
- Identify training requirements and provide both training materials (documentation and videos) and classroom instruction.

Within 30 days after award of optional CLIN the contractor must submit:

1. A draft POAM for the total integration of the AIMS Application. The POAM must include the timeline, milestones, and risks in the SMMS and RCMS-G project management plan.
2. A draft detailed WBS that outlines all work items and resources needed to successfully complete the project.

Within 10 Business days after receiving government feedback

1. A Government-approved final POAM (Section F, Deliverable 60)
2. A Government-approved final WBS (Section F, Deliverable 61)
3. Government-approved interim updates to the WBS and POAM as changes occur

C.5.17.1 Scope

The scope of the Army Incentive Management System should include the functionality necessary to:

- Prevent waste, fraud, and abuse.
- Provide for evaluating and recommending incentive options for Soldiers.
- Ensure more automated, efficient, and accurate processing of contracts and payments.
- Centralize storage and management of all incentive data.
- Improve oversight and ensure compliance with any future AAA and GAO audits.

The scope of functionality is best expressed with respect to the various centers and tools to be implemented in the Army Incentive Management Subsystem. Existing government-owned software can be leveraged to minimize the time necessary for implementation of these centers and tools. Analysis was conducted to assess whether the tools described below, which are currently implemented in the solution, could be subsumed by the Integrated Personnel and Pay System-Army (IPPS-A), and the decision was made that these tools are out of scope for IPPS-A and that RIMS will be a feeder system to IPPS-A providing all the management controls of a Soldiers incentives eligibility to IPPS-A.

C.5.17.2 Management Center

The management center must contain work buckets that allow for the management of contracts, payments, and Exceptions to Policy (ETP).

Work buckets must be automatically populated with contracts and payments across the following phases:

- Issue Phase
- Establish Control Phase
- Monitor Phase
- Payment Phase

Work buckets must also be available to manage ETP across their entire lifecycle. An ETP can be created by users with

system controls to ensure complete and appropriate ETP requests are submitted.

C.5.17.3 Administration Center

The Administration Center must provide the ability for designated users to conduct administrative activities discussed in the below modules.

- Law, Regulation, and Policy (LRP) Module
- Exception to Policy (ETP) Module
- Notification System Module
- Readiness Predictability Model (RPM) Module
- Unit Management Suite (UMS) Module

C.5.17.4 Information Center

A Policy Library within the Information Center must allow users to access system documentation, learning content (user's manuals, help guides, training videos, and other documentation) as deemed appropriate. It must also allow designated users to manage the content within the Information Center.

C.5.17.5 Budget Center

The Budget Center must allow designated users to manage funds within the given budget. Funds can be viewed by the incentive program based on being funded (total funding for the program), committed (contracts issued and active), obligated (contracts awaiting payment), and executed (payments made). Funds must be able to be moved between incentive programs as appropriate and necessary for current and out years. The budget module must provide the basis for evaluating current and out year funding at the point a contract is issued to ensure that funds for the contract are and should be available. Reports must also be available within the Budget Center.

The Budget Center must consist of:

- Budget Management Control (BMC) Module
- Budget Predictability Model (BPM) Module

C.5.17.6 User Management Tool (UMT)

UMTallows designated users to view requests for access to the Army Incentive Management Subsystem and requests for upgraded user roles and command levels. These users must be able to approve or disapprove requests as appropriate. Designated users must also be able to amend requests to appropriate roles or command levels as they deem appropriate. A history of all actions taken on a user account must be available to designated users, and reports must be available to view. UMT must contain the Active Component's Command Hierarchy to allow for full drill down capability from the highest level to the lowest level. Within UMT, the Command Hierarchy only allows users within the Soldier's command, or its command structure, to have access to actions for that Soldier.

C.5.17.7 Reporting Center

The Reporting Center must allow designated users to view standard reports and dashboards containing predefined data elements to monitor and aid in decision support for Army incentive programs. The Reporting Center must also allow designated users full access to all key data elements necessary to create ad hoc reports. Additionally, report subscriptions must allow for users to proactively obtain reports and dashboards through email at a frequency the user can define.

C.5.17.8 Search Tool

Users must be able to search for Soldiers and contracts. Soldier attributes including Social Security Number (SSN), DoDID (also referred to as EDIPI), Last Four, Full Name, Last Name, First Name, Rank, Mailing Zip Code, Unit State, Unit Processing Code (UPC), Currently Deployed, In Strength, and other designated attributes should narrow Soldier search results. Contract attributes including Contract Type, Control Number, Full Name, Rate Code, Contract

Start Date, Contract End Date, Stipend Start Date, Stipend End Date, Contract Signature Date, Issue Date, Expiration Term of Service (ETS) Date, Mandatory Removal Date (MRD), Unit State, UPC, Current Workflow Status, Current Workflow State, and other designated attributes should narrow contract search results.

C.5.17.9 Client Configuration Tool (CCT)

The Client Configuration Tool must allow designated users to make configuration changes to workflows, policies, dynamic generated addendums, and memos.

C.5.17.10 Soldier Center

The Soldier Center must allow every Soldier in the Army to login to check the status of their incentive contract and payment. The Soldier Center must allow the ability to request for an incentive that would then be routed to an approval authority. The Soldier Center must allow the ability to request for an inquiry if there is a problem with their incentive that will be routed to their Unit Administrator or reviewing authority. The Soldier Center must allow the ability for a Soldier with loan repayment to add loan records, disbursement records, upload supporting documents, and generate a DD2475 in support of their annual loan repayment incentive.

C.5.17.11 Requirements

The Army Incentive Management Subsystem must:

1. Provide multi-module automated support for bonus and incentive programs.
2. Guard against fraud, waste, and abuse, through the system's management and internal controls
3. Leverage a dimension data store
4. Provide automated support and management for Process Stakeholders/Roles.
5. Include multiple functional centers
6. Include an Exception to Policy (ETP) Module.
7. Include an Administrative Correction Request (ACR) Module.
8. Include an Incentives Termination Module.
9. Include workflows for each Bonus Type by Contract Phase.
10. Include workflows for each Regular Army Loan Repayment Program (RALRP) Type by Contract Phase.
11. Include workflows for each GI Bill Program Type by Contract Phase.
12. Include System Interface Agreements (SIAs).

C.5.17.12 Data

This task will require the contractor to establish a comparable Data Warehouse to the existing SMMS DW that establishes all required data to feed this new AIMS application. This DW will need to contain the Active Component of the Army and all relevant data to manage incentives. This new DW will be hosted with the ARNG DW, but must be severable. It will require the same standards of data processing procedures and operations that exist for TASK 2 and Task 3, only with the Active Army's data.

C.5.18 TASK 17 –AIMS OPERATIONS AND MAINTENANCE (OPTIONAL)

This task will only be turned on after the successful implementation of Task 16. The operations and support activities will be reported with all other applications on the MSR, and the support requirements must comply with all security and operational requirements IAW DoD, Army, other applicable government organizations, and this statement of work. Since this is scheduled to be a new implementation of existing software and business function, an estimated change request cannot be ascertained from historical data. It can however be assumed that at least 200 MCRs and SCRs will be required during the first year of this maintenance above the estimates stated in Task 6. It is likely that this will be reduced after the initial year of operations. This Maintenance must be tracked and managed separately from all other maintenance, however must be performed at the same quality, technical, and security standards as other required software and system maintenance tasks in the SOW.